A Quick Dip into MuddyWater's Recent Activity

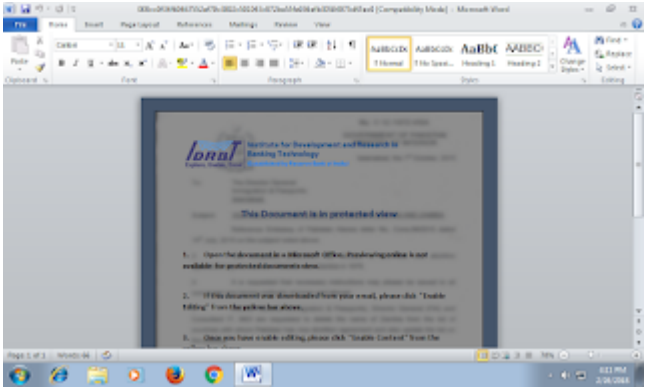
By Mo Bustami

Published: 2018-03-01 · Archived: 2026-04-05 23:21:06 UTC

A Quick Dip into MuddyWater's Recent Activity

INTRODUCTION

Since my last blog-post on MuddyWater operations, they seem to have been continuing their activities and as expected developing/changing some of their tactics and techniques. It is still apparent their heavy focus on layered obfuscation and preference for PowerShell. However, I will highlight what changed based on the sample that I will be analyzing.
This started with the sample "idrbt.doc" - 009cc0f34f60467552ef79c3892c501043c972be55fe936efb30584975d45ec0 uploaded to VT on February 27, 2017.



IDRBT stands for Institute for Development and Research in Banking Technology which according to Wikipedia is an institution exclusively focused on Banking Technology. Established by the Reserve Bank of India (RBI) in 1996, the Institution works at the intersection of Banking and Technology. It is located in Hyderabad, India. Right from carrying out cutting-edge Development and Research, enabling creation of technology infrastructure to moulding the technology talent required for Banking Sector, the institution enables technology transformation of the Indian Banking and Financial Sector.

Looking at this lure document might give you an indication of potential targets that the group might be focusing in this wave.

IS THAT SCRIPTLET I SEE??

My focus in this blog is to look at what changed in terms of the techniques used by the group to achieve their objective which can be summarized as the following:

1. The lure document mentioned above is delivered as a password protected document. This is probably to try and evade some of the automated analysis tools that some of the target might have in place.
2. Increase the level of obfuscation in the embedded macro as it now contains:
    - Base64 encoding scattered across the macro code and in some cases double Base64 encoded is used.
    - Use of XoR in the macro code to create the commands to be executed by running the macro.
    - The use of a publicly available code to potentially bypass AppLocker via the use of *"csmtp.exe"* or in this case using csmtp to execute scriptlet files which will in turn run a PowerShell code known as the MuddyWater PowerShell payload (*POWERSTATS*). The POWERSTATS variant in this case is originally Base64 encoded within the Macro.

    - Additional layering of obfuscated PowerShell to make analysis hard when looking at the PowerShell code. In this case the PowerShell script is heavily obfuscated with character replacement functions (I counted 5 layers at least) with the layering of obfuscation being focused on the PowerShell script portion related to the Proxy servers which has risen to over 900 servers (Provided at the bottom as part of the IoCs) - Please keep in mind that most of these might be representing compromised sites.

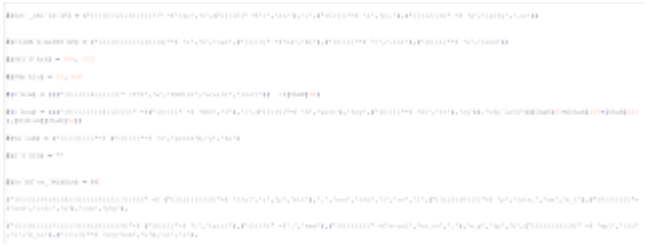
OBFUSCATE OBFUSCATE OBFUSCATE

The POWERSTATS payload that this group relies on is heavily obfuscated. The code is first embedded within the macro code as a double Base64 encoded variable.

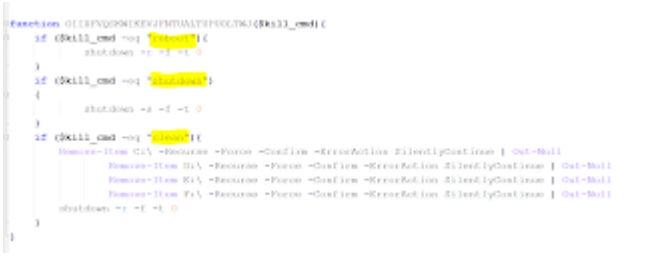
Once decoded you will be presented with the more familiar Invoke-Expression/Invoke/Obfuscation PowerShell script that MuddyWater relies on.

As previous iterations of POWERSTATS, the script is split into three parts:

- Script responsible for the Proxy Server, IP Location of the victim, Filename Path, etc. Similar to the variant used in the [BurpSuite KeyGen], the variable responsible to store the proxy values is names *"Dragon Middle"*.

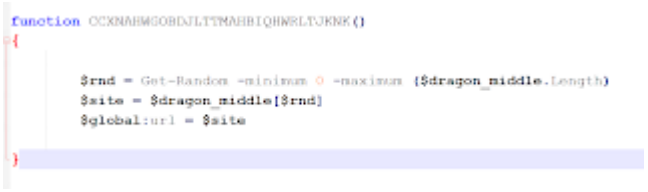


- Script that is the core code of the payload which contains the functions for multiple commands including:
    - Kill command (Reboot, Shutdown or Clean)



    - Message encryption function

    - URL proxy function



```
function CCKNAHMGOBDJLTTMAHBIQHWRLYJKNK()
{

    $rnd = Get-Random -minimum 0 -maximum ($dragon_middle.Length)
    $site = $dragon_middle[$rnd]
    $global:url = $site

}
```

    - Function that include command to take screenshots

- Persistence Function.

- What seems to be Lateral Movement functions leveraging either DDEInitiate on Excel, CreateObject on Outlook and ShellWindows “Document.Application.ShellExecute” all via DCOM. You can find the methods used taken from this blog, this blog, this script and this blog. - *I could be wrong but I thing this is a new piece of code/function added compared to earlier samples I looked at.*

- Sleep and Anti Analysis functions

- Upload Function

- The third script portion is focused on the encryption and decryption between the C&C and the victim

INTERESTING STRINGS

As part of analyzing the document, I came across some interesting strings. In particular, the document included this string *"CMG = "21238DCB91CB91CE96CE96*"". Googling this string returns only 3 results directing to the following sites:

- *hxxp://www[.]hnydjz[.]com/module/download/downfile.jsp?classid=0&filename=139bf1d94eb646fcbd44de40ce2163d7.doc*
- *hxxp://www[.]liketoshow[.]com/module/download/downfile.jsp?classid=0&filename=139bf1d94eb646fcbd44de40ce2163d7.doc*
- *hxxp://www[.]cn93[.]org/xxgk/jcms_files/jcms1/web107/site/zfxxgk/download/downfile.jsp?filename=171207081414203.doc*

As of the writing of this blog, all three links seem to redirect to just a web page rather a DOC file. However, looking at some cached results for the third link, The page looked interesting as it contained further interesting strings within it:

- *"\rjoawork.bak"* - this seems to be scattered within the results and further researching this string on Google, it yields about ~40 results which all seem to be DOC related and with Chinese focus.
- *"Module=RJeGov"* - This is the same as the above however this returns further results of about ~240.

I actually do not know if this is anything or if I stumbled upon anything related or not but it just seems interesting to me. One thing to notice that most of the returned results seems to be Chinese sites.

FINAL THOUGHTS

This continues to shows that MuddyWater group are continuously evolving their techniques. Again, the different lures and methods used by this group continue to show that they might have a wide focus on multiple verticals and industries.
Below you will find a list of IoCs from my analysis and I am sure others will be able to dig deeper into this an uncover further details. Hope this is of help and benefit.

INDICATORS OF COMPROMISE

HASHES

009cc0f34f60467552ef79c3892c501043c972be55fe936efb30584975d45ec0
288afbe21d69e79a1cff44e2db7f491af10381bcc54436a8f900bcbd2a752a6f
c87799cce6d65158da97aa31a5160a0a6b6dd5a89dea312604cc66ed5e976cc9

PROXY LIST

hxxp://alessandrofoglino[.]com//db_template.php
hxxp://www.easy-home-sales.co.za//db_template.php
hxxp://www.almaarefut[.]com/admin/db_template.php
hxxp://chinamall.co.za//db_template.php
hxxp://amesoulcoaching[.]com//db_template.php
hxxp://www.antigonisworld[.]com/wp-includes/db_template.php
hxxps://anbinni.ba/wp-admin/db_template.php
hxxp://arctistrade.de/wp/db_template.php

hxxp://aianalytics.ie//db_template.php
hxxp://www.gilforsenate[.]com//db_template.php
hxxp://mgamule.co.za/oldweb/db_template.php
hxxp://chrisdejager-attorneys.co.za//db_template.php
hxxp://alfredocifuentes[.]com//db_template.php
hxxp://alxcorp[.]com//db_template.php
hxxps://www.aircafe24[.]com//db_template.php
hxxp://agencereferencement.be/wp-admin/db_template.php
hxxp://americanlegacies.org/webthed_ftw/db_template.php
hxxps://aloefly.net//db_template.php
hxxp://www.duotonedigital.co.za//db_template.php
hxxp://architectsinc.net//db_template.php
hxxp://www.tanati.co.za//db_template.php
hxxp://emware.co.za//db_template.php
hxxp://breastfeedingbra.co.za//db_template.php
hxxp://alhidayahfoundation.co.uk/category/db_template.php
hxxp://cashforyousa.co.za//db_template.php
hxxps://www.airporttaxi-uk.co.uk/wp-includes/db_template.php
hxxp://antjetaubert.de//db_template.php
hxxp://hesterwebber.co.za//db_template.php
hxxp://fickstarelectrical.co.za//db_template.php
hxxp://alex-frost[.]com/assets/db_template.php
hxxps://americanbrasil[.]com.br//db_template.php
hxxps://aileeshop[.]com//db_template.php
hxxps://annodle[.]com//db_template.php
hxxp://goldeninstitute.co.za/contents/db_template.php
hxxp://ednpk[.]com//db_template.php
hxxp://www.arabiccasinochoice[.]com//db_template.php
hxxp://proeventsports.co.za//db_template.php
hxxp://glenbridge.co.za//db_template.php
hxxp://berped.co.za//db_template.php
hxxp://best-digital-slr-cameras[.]com//db_template.php
hxxp://antonhirvonen[.]com/pengalandet.se/wp-includes/db_template.php
hxxp://www.alpacal[.]com//db_template.php
hxxps://www.alakml[.]com/wp-admin/db_template.php
hxxp://ar-rihla[.]com//db_template.php
hxxp://appsvoice.info//db_template.php
hxxp://www.bashancorp.co.za//db_template.php
hxxp://alexanderbecker.net/services/db_template.php
hxxp://visionclinic.co.ls/visionclinic/db_template.php
hxxps://www.angelesrevista[.]com//db_template.php
hxxps://www.antojoentucocina[.]com//db_template.php

hxxp://apollonweb[.]com//db_template.php
hxxps://www.alphapixa[.]com//db_template.php
hxxp://capitalradiopetition.co.za//db_template.php
hxxp://www.generictoners.co.za//db_template.php
hxxps://alnahdatraining[.]com//db_template.php
hxxps://albousala[.]com//db_template.php
hxxps://www.dopetroleum[.]com//db_template.php
hxxp://bios-chip.co.za//db_template.php
hxxp://www.crissamconsulting.co.za//db_template.php
hxxp://capriflower.co.za//db_template.php
hxxp://www.dingaanassociates.co.za//db_template.php
hxxp://indiba-africa.co.za//db_template.php
hxxp://verifiedseller.co.za/js/db_template.php
hxxps://www.buraqlubricant[.]com//db_template.php
hxxp://aqarco[.]com/wp-admin/db_template.php
hxxp://allaboutblockchain.net//db_template.php
hxxp://www.amexcars.info/tpl/db_template.php
hxxp://clandecor.co.za/rvsUtf8Backup/db_template.php
hxxp://bakron.co.za//db_template.php
hxxp://gsnconsulting.co.za//db_template.php
hxxp://vumavaluations.co.za//db_template.php
hxxp://heritagetravelmw[.]com//db_template.php
hxxp://ampvita[.]com//db_template.php
hxxp://ahero-resource-center.org/administrator/db_template.php
hxxps://arbulario[.]com//db_template.php
hxxp://havilahglo.co.za/wpscripts/db_template.php
hxxp://www.bestdecorativemirrors[.]com/More-Mirrors/db_template.php
hxxp://delectronics[.]com.pk//db_template.php
hxxp://antucomp[.]com//db_template.php
hxxp://advocatetn[.]com/font-awesome/fonts/db_template.php
hxxps://amooy[.]com/webservice/db_template.php
hxxp://www.harmonyguesthouse.co.za//db_template.php
hxxp://alanrori[.]com//db_template.php
hxxp://algarvesup[.]com//db_template.php
hxxp://desirablehair.co.za//db_template.php
hxxp://comsip.org.mw//db_template.php
hxxp://jdcorporate.co.za/catalog/db_template.php
hxxp://andrewfinnburhoe[.]com//db_template.php
hxxp://anyeva[.]com/wp-includes/db_template.php
hxxp://www.agenceuhd[.]com//db_template.php
hxxp://host4unix.net/host24new/db_template.php
hxxp://www.altaica.ca/wordpress/db_template.php

hxxp://www.allbuyer.co.uk//db_template.php
hxxp://jvpsfunerals.co.za//db_template.php
hxxp://immaculatepainters.co.za//db_template.php
hxxp://tcpbereka.co.za/js/db_template.php
hxxp://clientcare.co.ls//db_template.php
hxxp://investaholdings.co.za/htc/db_template.php
hxxp://www.amjobs.co.uk//db_template.php
hxxp://www.agirlgonewine[.]com/store/db_template.php
hxxp://findinfo-more[.]com//db_template.php
hxxp://asgen.org//db_template.php
hxxp://alphasalesrecruitment[.]com//db_template.php
hxxp://irshadfoundation.co.za//db_template.php
hxxp://analternatif[.]com/includes/db_template.php
hxxp://arbruisseau[.]com/profiles/db_template.php
hxxp://ladiescircle.co.za//db_template.php
hxxp://all-reseller[.]com/zzz_backup/db_template.php
hxxp://alcatrazmoon[.]com/images/db_template.php
hxxp://www.alcalumni[.]com/wp-includes/db_template.php
hxxp://aniljoseph[.]com/servermon/db_template.php
hxxp://alwake3press[.]com/wp-includes/db_template.php
hxxp://www.hfhl.org.ls/habitat/db_template.php
hxxp://alcafricanos[.]com/slsmonographs/db_template.php
hxxps://agapeencounter.org//db_template.php
hxxp://apobiomedix.ca//db_template.php
hxxp://anythinglah.info//db_template.php
hxxp://aniroleplay.net//db_template.php
hxxp://www.allcopytoners[.]com//db_template.php
hxxp://alphaobring[.]com//db_template.php
hxxp://www.galwayprimary.co.za//db_template.php
hxxp://alnuzha.org/en/db_template.php
hxxps://ancient-wisdoms[.]com//db_template.php
hxxp://amazingenergysavings.net//db_template.php
hxxp://gvs[.]com.pk/font-awesome/db_template.php
hxxp://geetransfers.co.za/font-awesome/db_template.php
hxxp://carlagrobler.co.za/components/db_template.php
hxxp://amazingashwini[.]com//db_template.php
hxxp://aminearserver.es//db_template.php
hxxp://lensofafrica.co.za//db_template.php
hxxp://greenacrestf.co.za/video/db_template.php
hxxp://www.tonaro.co.za//db_template.php
hxxp://alephit2.biz/kitzz/db_template.php
hxxp://lppaportal.org.ls//db_template.php

hxxp://alkousy[.]com//db_template.php
hxxp://ambulatorioveterinariocalusco[.]com/img/common/db_template.php
hxxp://fragranceoil.co.za//db_template.php
hxxp://www.eloquent.co.za/nweb2/db_template.php
hxxp://chrishanicdc.org/wpimages/db_template.php
hxxp://ahc.me.uk//db_template.php
hxxp://www.britishasia-equip.co.uk//db_template.php
hxxp://always-beauty.ch//db_template.php
hxxps://www.ancamamara[.]com/wp-admin/db_template.php
hxxp://entracorntrading.co.za//db_template.php
hxxp://www.alexjeffersonconsulting[.]com/wp-includes/db_template.php
hxxp://americabr[.]com.br//db_template.php
hxxp://andrew-snyder.net/bootstrap/db_template.php
hxxp://signsoftime.co.za//db_template.php
hxxp://aperta-armis.org//db_template.php
hxxp://absfinancialplanning.co.za/images/db_template.php
hxxp://charispaarl.co.za//db_template.php
hxxp://indlovusecurity.co.za//db_template.php
hxxp://alcafricandatalab[.]com//db_template.php
hxxp://amor-clubhotels[.]com//db_template.php
hxxp://mokorotlocorporate[.]com//db_template.php
hxxp://appriori[.]com//db_template.php
hxxp://luxconprojects.co.za//db_template.php
hxxp://androidphonetips[.]com/wp-includes/db_template.php
hxxp://angel-seeds[.]com.ua/catalog/db_template.php
hxxp://alissanicolai[.]com/assets/db_template.php
hxxps://www.amateurastronomy.org//db_template.php
hxxp://aiofotoevideo[.]com//db_template.php
hxxp://www.amika.hr//db_template.php
hxxp://comfortex.co.za/php/db_template.php
hxxp://deepgraphics.co.za//db_template.php
hxxps://agiledepot[.]com//db_template.php
hxxp://almatours.gr//db_template.php
hxxp://analystcnwang[.]com//db_template.php
hxxp://www.malboer.co.za/trendy1/db_template.php
hxxp://sefikengfarm.co.ls//db_template.php
hxxp://www.antirughenaturale[.]com/wp-admin/db_template.php
hxxp://passright.co.za//db_template.php
hxxp://seismicfactory.co.za//db_template.php
hxxp://alessandroalessandrini.it//db_template.php
hxxps://aquabsafe[.]com//db_template.php
hxxp://amatikulutours[.]com/tmp/db_template.php

hxxp://ganitis.gr//db_template.php
hxxp://aleenasgiftbox[.]com/admin/db_template.php
hxxps://allusdoctors[.]com/themes/db_template.php
hxxp://alainsaffel[.]com//db_template.php
hxxp://www.ariehandomri[.]com//db_template.php
hxxp://aquaneeka.co.uk/wp-includes/db_template.php
hxxp://itengineering.co.za/gatewaydiamond/db_template.php
hxxp://alldomains-crm[.]com/bubblegumpopcorn[.]com/wp-admin/db_template.php
hxxp://www.albertamechanical.ca//db_template.php
hxxp://alchamel.info//db_template.php
hxxps://almokan.net/wp-includes/db_template.php
hxxp://jakobieducation.co.za//db_template.php
hxxps://arc-sec.net//db_template.php
hxxp://ldams.org.ls/supplies/db_template.php
hxxp://menaboracks.co.za/tmp/db_template.php
hxxp://www.getcord.co.za//db_template.php
hxxp://boardaffairs[.]com//db_template.php
hxxp://capetownway.co.za//db_template.php
hxxp://cloudhostdesign[.]com//db_template.php
hxxp://hartenboswaterpark.co.za/templates/db_template.php
hxxp://fccorp.co.za/php/db_template.php
hxxp://angar68[.]com//db_template.php
hxxp://www.dws-gov.co.za//db_template.php
hxxp://alwahahweb[.]com//db_template.php
hxxp://anuragcreatives[.]com//db_template.php
hxxp://embali.co.za//db_template.php
hxxp://albertaedmonton[.]com/widgetstyles/db_template.php
hxxp://altosdefontana[.]com//db_template.php
hxxp://airfanhydro.net//db_template.php
hxxps://www.alexponcet[.]com/wp-includes/db_template.php
hxxp://agropecuariavilarica[.]com.br//db_template.php
hxxps://www.amazingbuyrd[.]com/admin/db_template.php
hxxp://cdxtrading.co.za//db_template.php
hxxp://interafricaconsulting[.]com/wpimages/db_template.php
hxxp://glgroup.co.za/images/db_template.php
hxxp://hisandherskennels.co.za/php/db_template.php
hxxp://alemaohost[.]com/lotosorg[.]com/db_template.php
hxxp://isibaniedu.co.za/admin/db_template.php
hxxp://dianakleyn.co.za/layouts/db_template.php
hxxp://themotoringcalendar.co.za//db_template.php
hxxp://www.loansonhomes.co.za//db_template.php
hxxp://edgesecurity.co.za/js/db_template.php

hxxp://highschoolsuperstar.co.za/files/db_template.php
hxxp://www.ambientproperty[.]com//db_template.php
hxxp://animationshowreel.co.il//db_template.php
hxxp://cafawelding.co.za/font-awesome/db_template.php
hxxp://apalawyers.pt//db_template.php
hxxp://www.edesignz.co.za//db_template.php
hxxp://centuryacademy.co.za/css/db_template.php
hxxps://ambyenta.hr//db_template.php
hxxp://ceramica.co.za//db_template.php
hxxp://www.alfredoposada[.]com//db_template.php
hxxp://anastasovsworkshop[.]com/wp-includes/db_template.php
hxxp://allisonplumbing[.]com/wp-includes/db_template.php
hxxp://eastrandmotorlab.co.za/fleet/db_template.php
hxxp://angelsongroup[.]com/wp-includes/db_template.php
hxxp://www.mikimaths[.]com//db_template.php
hxxp://hjb-racing.co.za/htdocs/db_template.php
hxxp://anotherpartofme[.]com/wp-includes/db_template.php
hxxp://www.andreabelfi[.]com//db_template.php
hxxp://www.iancullen.co.za//db_template.php
hxxp://alaskamaterials[.]com//db_template.php
hxxp://jeanetteproperties.co.za//db_template.php
hxxp://www.digitalmedia.co.za//db_template.php
hxxp://www.rejoicetheatre[.]com//db_template.php
hxxps://alterwebhost[.]com//db_template.php
hxxp://bc-u.co.uk//db_template.php
hxxp://dpscdgkhan.edu.pk/shopping/db_template.php
hxxp://edgeforensic.co.za//db_template.php
hxxp://willpowerpos.co.za//db_template.php
hxxp://antrismode[.]com/wp-includes/db_template.php
hxxp://colenesphotography.co.za/modules/db_template.php
hxxp://anthaigroup.vn//db_template.php
hxxps://alphainvestors[.]com.au//db_template.php
hxxps://aliart.nl//db_template.php
hxxps://allmantravel[.]com/thumbs/db_template.php
hxxp://fbrvolume.co.za//db_template.php
hxxp://amordegato.es/storefront/db_template.php
hxxp://agylub[.]com//db_template.php
hxxp://www.khotsonglodge.co.ls//db_template.php
hxxp://ampli5yd[.]com//db_template.php
hxxps://animeok.co.il//db_template.php
hxxps://arbeidsrechtcentrum.nl//db_template.php
hxxp://erniecommunications.co.za/js/db_template.php

hxxp://promechtransport.co.za/scripts/db_template.php
hxxp://centuriongsd.co.za//db_template.php
hxxp://www.agencesylvieleclerc[.]com//db_template.php
hxxp://delcom.co.za//db_template.php
hxxps://aleoestudio[.]com/gallonature/db_template.php
hxxp://oftheearthphotography[.]com/www/db_template.php
hxxp://h-dubepromotions.co.za//db_template.php
hxxp://www.alessioborzuola[.]com/downloads/db_template.php
hxxp://crystaltidings.co.za//db_template.php
hxxp://funeralbusinesssolution[.]com/email_template/db_template.php
hxxp://funisalodge.co.za/data1/db_template.php
hxxp://experttutors.co.za//db_template.php
hxxps://www.cartridgecave.co.za//db_template.php
hxxp://ecs-consult[.]com//db_template.php
hxxp://www.animationinisrael.org/tmp_images/db_template.php
hxxp://gideonitesprojects[.]com//db_template.php
hxxp://hybridauto.co.za/photography/db_template.php
hxxp://africanpixels.zar.cc//db_template.php
hxxp://ryanchristiefurniture.co.za//db_template.php
hxxp://evansmokaba[.]com/evansmokaba[.]com/thabiso/db_template.php
hxxp://almeriahotelja[.]com/dk/db_template.php
hxxp://al3abflash.biz//db_template.php
hxxp://www.fun4kidz.co.za//db_template.php
hxxp://alsharhanstore[.]com//db_template.php
hxxp://www.infratechconsulting[.]com//db_template.php
hxxp://algihad[.]com/assets/db_template.php
hxxp://americanwestmedia[.]com//db_template.php
hxxp://charliewestsecurity.co.za//db_template.php
hxxp://beehiveholdingszar.co.za//db_template.php
hxxp://analyticalfootball[.]com//db_template.php
hxxp://apiiination[.]com/leadership/db_template.php
hxxps://ahelicoptermom[.]com/wp-includes/db_template.php
hxxp://servicebox.co.za//db_template.php
hxxp://globalelectricalandconstruction.co.za/wpscripts/db_template.php
hxxps://aquo.in//db_template.php
hxxps://www.alfransia[.]com/wp-admin/db_template.php
hxxp://www.icsswaziland[.]com//db_template.php
hxxp://aiko.pro//db_template.php
hxxps://alceharfield[.]com//db_template.php
hxxp://indocraft.co.za/test/db_template.php
hxxp://allegiancesecurity.org//db_template.php
hxxp://sullivanprimary.co.za//db_template.php

hxxp://www.apmequestrian[.]com//db_template.php
hxxps://alphawaves.org/wp-admin/db_template.php
hxxp://www.alexandrasternin[.]com/illustration/db_template.php
hxxp://www.daleth.co.za//db_template.php
hxxp://jwseshowe.co.za/assets/db_template.php
hxxp://winagainstebola[.]com//db_template.php
hxxp://anubandh.in//db_template.php
hxxp://www.alexanderhomestead[.]com//db_template.php
hxxp://alfatek-intelligence[.]com//db_template.php
hxxp://www.aprendiendoencasa[.]com/wp-includes/db_template.php
hxxp://alorabrownies[.]com/wp-admin/db_template.php
hxxp://andrasadam[.]com/tothildiko/wp-includes/db_template.php
hxxp://cazochem.co.za/cazochem/db_template.php
hxxp://debnoch[.]com/image/db_template.php
hxxp://hmholdings360.co.za//db_template.php
hxxp://iinvest4u.co.za//db_template.php
hxxp://burgercoetzeeattorneys.co.za//db_template.php
hxxp://anngrigphoto[.]com//db_template.php
hxxp://alchemistasonida[.]com//db_template.php
hxxp://anahera.biz/admin/db_template.php
hxxp://h-u-i.co.za/heiren/db_template.php
hxxp://insta-art.co.za//db_template.php
hxxp://muallematsela[.]com//db_template.php
hxxp://aguasdecastilla[.]com/uploads/db_template.php
hxxp://www.arabgamenetwork[.]com//db_template.php
hxxps://arhiepiscopiabucurestilor.ro/templates/db_template.php
hxxp://amruthavana[.]com/blog/db_template.php
hxxp://digitalblue.co.za//db_template.php
hxxps://www.alvarezarquitectos[.]com//db_template.php
hxxp://buboobioinnovations.co.za/wpimages/db_template.php
hxxp://andrewsbisom[.]com//db_template.php
hxxp://www.m-3.co.za//db_template.php
hxxp://beesrenovations.co.za/images/db_template.php
hxxps://www.apliety.co.il/wp-includes/db_template.php
hxxp://alchamelup.org/htdocs/db_template.php
hxxp://benonicoc.co.za/resources/db_template.php
hxxps://al-mostakbl[.]com//db_template.php
hxxp://alchimiegrafiche.net/bbdelteatro/db_template.php
hxxp://andrespazsoldan[.]com//db_template.php
hxxp://in2accounting.co.za//db_template.php
hxxp://aipa.ca//db_template.php
hxxp://alphabee.fund/PHPMailer_5.2.0/db_template.php

hxxp://arabsdeals[.]com//db_template.php
hxxps://archiotronic[.]com/wp-includes/db_template.php
hxxp://capewindstrading.co.za//db_template.php
hxxps://althurayaa[.]com//db_template.php
hxxp://jhphotoedits.co.za//db_template.php
hxxp://cloudhub.co.ls/modules/db_template.php
hxxp://apironco[.]com/wp-includes/db_template.php
hxxp://digital-cameras-south-africa.co.za/script/db_template.php
hxxp://ahmadhasanat[.]com//db_template.php
hxxp://alexrocchi[.]com//db_template.php
hxxp://aljaadi[.]com//db_template.php
hxxps://www.engeltjieakademie.co.za//db_template.php
hxxp://annabelle.nl/next/db_template.php
hxxp://juniorad.co.za/vendor/db_template.php
hxxp://animationpulse.net//db_template.php
hxxp://angloglot[.]com//db_template.php
hxxp://agricolavicuna.cl//db_template.php
hxxp://alexelgy[.]com/allaccess/db_template.php
hxxp://www.centreforgovernance.uk//db_template.php
hxxp://www.aliandconsulting[.]com//db_template.php
hxxp://balaateen.co.za/less/db_template.php
hxxp://aleksicdunja[.]com//db_template.php
hxxp://arestihome[.]com//db_template.php
hxxp://am1int.fcomet[.]com/wp1/db_template.php
hxxp://anet-international-group[.]com/shop/db_template.php
hxxp://courtesydriving.co.za/js/db_template.php
hxxp://annaplebanek[.]com//db_template.php
hxxp://agencijazemil[.]com//db_template.php
hxxp://airminumtiro[.]com//db_template.php
hxxp://www.androidwikihow[.]com//db_template.php
hxxp://alisabyfinna[.]com//db_template.php
hxxp://rma-law.co.za//db_template.php
hxxp://amari.ro/components/db_template.php
hxxp://anxiousandunstoppable[.]com//db_template.php
hxxp://www.buhlebayoacademy[.]com//db_template.php
hxxp://arabellajo[.]com/wp/wp-includes/db_template.php
hxxp://blackthorn.co.za//db_template.php
hxxp://alaqaba[.]com/dnsarabia[.]com/db_template.php
hxxp://airesis.blog/wp-admin/db_template.php
hxxp://www.aptibet.org//db_template.php
hxxp://alecattic[.]com/wp-includes/db_template.php
hxxp://anglero[.]com//db_template.php

hxxp://getabletravel.co.za/wpscripts/db_template.php
hxxp://www.allwestdental[.]com/wp-includes/db_template.php
hxxp://printernet.co.za//db_template.php
hxxp://genesisbs.co.za//db_template.php
hxxp://allsporthealthandfitness[.]com//db_template.php
hxxp://www.humorcarbons[.]com//db_template.php
hxxp://intelligentprotection.co.za//db_template.php
hxxp://amazethings[.]com//db_template.php
hxxp://incoso.co.za/images/db_template.php
hxxp://www.antoanetapalikarska[.]com//db_template.php
hxxps://www.alteaparadise[.]com/wp-includes/db_template.php
hxxp://amirmenahem[.]com//db_template.php
hxxp://isound.co.za//db_template.php
hxxp://www.alestilorachel[.]com//db_template.php
hxxp://alcfm.net/wp-admin/db_template.php
hxxp://www.acer-parts.co.za//db_template.php
hxxp://www.gsmmid[.]com//db_template.php
hxxp://skhaleni.co.za//db_template.php
hxxps://amiici.vision//db_template.php
hxxps://andihaas.at/wp-includes/db_template.php
hxxp://www.albertaprimebeef[.]com//db_template.php
hxxps://www.appster.it/wp-includes/db_template.php
hxxp://amofoundation.org/wp-includes/db_template.php
hxxp://iqra.co.za/pub/db_template.php
hxxp://thecompasssolutions.co.za//db_template.php
hxxp://archwaycarpetscrm.co.uk//db_template.php
hxxp://iggleconsulting[.]com//db_template.php
hxxps://angel-blanco.net/wp-includes/db_template.php
hxxps://anotherdayinparadise.ca//db_template.php
hxxp://www.bitp.co.za//db_template.php
hxxp://cupboardcure.co.za/vendor/db_template.php
hxxp://all2wedding[.]com/wp-includes/db_template.php
hxxp://allianz[.]com.pe/wp-admin/db_template.php
hxxp://amiehepperlin[.]com//db_template.php
hxxps://www.amighini.it/webservice/db_template.php
hxxp://broken-arrow.co.za//db_template.php
hxxp://www.ihlosiqs-pm.co.za//db_template.php
hxxp://alisimple.si/wp-includes/db_template.php
hxxp://allthat.social//db_template.php
hxxp://www.amphibiblechurch[.]com//db_template.php
hxxp://bestencouragementwords[.]com//db_template.php
hxxp://alayhamtechnologies[.]com//db_template.php

hxxps://alaskanharvestseafood[.]com/backup/db_template.php
hxxps://www.air-mag.ro//db_template.php
hxxp://get-paid-for-online-survey[.]com//db_template.php
hxxp://www.antc.ch/wp-includes/db_template.php
hxxp://firstchoiceproperties.co.za//db_template.php
hxxp://habibtextiles.pk//db_template.php
hxxp://fsproperties.co.za/engine1/db_template.php
hxxp://diegemmerkat.co.za//db_template.php
hxxp://molepetravel.co.ls//db_template.php
hxxp://mmetl.co.za//db_template.php
hxxp://altrablog[.]com//db_template.php
hxxp://abrahamseed.co.za//db_template.php
hxxp://www.amerindgen[.]com/author/admin1/db_template.php
hxxp://altcoinaddict[.]com//db_template.php
hxxp://iiee.edu.pk//db_template.php
hxxp://cmhts.co.za/resources/db_template.php
hxxp://domesticguardians.co.za/Banner/db_template.php
hxxps://amishcountryfurnishings[.]com//db_template.php
hxxps://allday.gr//db_template.php
hxxp://www.alinn-u-yin[.]com//db_template.php
hxxps://www.allin-chain[.]com//db_template.php
hxxps://www.anatapackaging[.]com/vendors/db_template.php
hxxp://alexcelts[.]com/wp/db_template.php
hxxp://www.allstylus[.]com.br//db_template.php
hxxp://www.algom-law[.]com//db_template.php
hxxp://ambiances-toiles.fr//db_template.php
hxxp://alessandrofoglino[.]com//db_template.php
hxxp://www.easy-home-sales.co.za//db_template.php
hxxp://www.almaarefut[.]com/admin/db_template.php
hxxp://chinamall.co.za//db_template.php
hxxp://amesoulcoaching[.]com//db_template.php
hxxp://www.antigonisworld[.]com/wp-includes/db_template.php
hxxps://anbinni.ba/wp-admin/db_template.php
hxxp://arctistrade.de/wp/db_template.php
hxxp://aianalytics.ie//db_template.php
hxxp://www.gilforsenate[.]com//db_template.php
hxxp://mgamule.co.za/oldweb/db_template.php
hxxp://chrisdejager-attorneys.co.za//db_template.php
hxxp://alfredocifuentes[.]com//db_template.php
hxxp://alxcorp[.]com//db_template.php
hxxps://www.aircafe24[.]com//db_template.php
hxxp://agencereferencement.be/wp-admin/db_template.php

hxxp://americanlegacies.org/webthed_ftw/db_template.php
hxxps://aloefly.net//db_template.php
hxxp://www.duotonedigital.co.za//db_template.php
hxxp://architectsinc.net//db_template.php
hxxp://www.tanati.co.za//db_template.php
hxxp://emware.co.za//db_template.php
hxxp://breastfeedingbra.co.za//db_template.php
hxxp://alhidayahfoundation.co.uk/category/db_template.php
hxxp://cashforyousa.co.za//db_template.php
hxxps://www.airporttaxi-uk.co.uk/wp-includes/db_template.php
hxxp://antjetaubert.de//db_template.php
hxxp://hesterwebber.co.za//db_template.php
hxxp://fickstarelectrical.co.za//db_template.php
hxxp://alex-frost[.]com/assets/db_template.php
hxxps://americanbrasil[.]com.br//db_template.php
hxxps://aileeshop[.]com//db_template.php
hxxps://annodle[.]com//db_template.php
hxxp://goldeninstitute.co.za/contents/db_template.php
hxxp://ednpk[.]com//db_template.php
hxxp://www.arabiccasinochoice[.]com//db_template.php
hxxp://proeventsports.co.za//db_template.php
hxxp://glenbridge.co.za//db_template.php
hxxp://berped.co.za//db_template.php
hxxp://best-digital-slr-cameras[.]com//db_template.php
hxxp://antonhirvonen[.]com/pengalandet.se/wp-includes/db_template.php
hxxp://www.alpacal[.]com//db_template.php
hxxps://www.alakml[.]com/wp-admin/db_template.php
hxxp://ar-rihla[.]com//db_template.php
hxxp://appsvoice.info//db_template.php
hxxp://www.bashancorp.co.za//db_template.php
hxxp://alexanderbecker.net/services/db_template.php
hxxp://visionclinic.co.ls/visionclinic/db_template.php
hxxps://www.angelesrevista[.]com//db_template.php
hxxps://www.antojoentucocina[.]com//db_template.php
hxxp://apollonweb[.]com//db_template.php
hxxps://www.alphapixa[.]com//db_template.php
hxxp://capitalradiopetition.co.za//db_template.php
hxxp://www.generictoners.co.za//db_template.php
hxxps://alnahdatraining[.]com//db_template.php
hxxps://albousala[.]com//db_template.php
hxxps://www.dopetroleum[.]com//db_template.php
hxxp://bios-chip.co.za//db_template.php

hxxp://www.crissamconsulting.co.za//db_template.php
hxxp://capriflower.co.za//db_template.php
hxxp://www.dingaanassociates.co.za//db_template.php
hxxp://indiba-africa.co.za//db_template.php
hxxp://verifiedseller.co.za/js/db_template.php
hxxps://www.buraqlubricant[.]com//db_template.php
hxxp://aqarco[.]com/wp-admin/db_template.php
hxxp://allaboutblockchain.net//db_template.php
hxxp://www.amexcars.info/tpl/db_template.php
hxxp://clandecor.co.za/rvsUtf8Backup/db_template.php
hxxp://bakron.co.za//db_template.php
hxxp://gsnconsulting.co.za//db_template.php
hxxp://vumavaluations.co.za//db_template.php
hxxp://heritagetravelmw[.]com//db_template.php
hxxp://ampvita[.]com//db_template.php
hxxp://ahero-resource-center.org/administrator/db_template.php
hxxps://arbulario[.]com//db_template.php
hxxp://havilahglo.co.za/wpscripts/db_template.php
hxxp://www.bestdecorativemirrors[.]com/More-Mirrors/db_template.php
hxxp://delectronics[.]com.pk//db_template.php
hxxp://antucomp[.]com//db_template.php
hxxp://advocatetn[.]com/font-awesome/fonts/db_template.php
hxxps://amooy[.]com/webservice/db_template.php
hxxp://www.harmonyguesthouse.co.za//db_template.php
hxxp://alanrori[.]com//db_template.php
hxxp://algarvesup[.]com//db_template.php
hxxp://desirablehair.co.za//db_template.php
hxxp://comsip.org.mw//db_template.php
hxxp://jdcorporate.co.za/catalog/db_template.php
hxxp://andrewfinnburhoe[.]com//db_template.php
hxxp://anyeva[.]com/wp-includes/db_template.php
hxxp://www.agenceuhd[.]com//db_template.php
hxxp://host4unix.net/host24new/db_template.php
hxxp://www.altaica.ca/wordpress/db_template.php
hxxp://www.allbuyer.co.uk//db_template.php
hxxp://jvpsfunerals.co.za//db_template.php
hxxp://immaculatepainters.co.za//db_template.php
hxxp://tcpbereka.co.za/js/db_template.php
hxxp://clientcare.co.ls//db_template.php
hxxp://investaholdings.co.za/htc/db_template.php
hxxp://www.amjobs.co.uk//db_template.php
hxxp://www.agirlgonewine[.]com/store/db_template.php

hxxp://findinfo-more[.]com//db_template.php
hxxp://asgen.org//db_template.php
hxxp://alphasalesrecruitment[.]com//db_template.php
hxxp://irshadfoundation.co.za//db_template.php
hxxp://analternatif[.]com/includes/db_template.php
hxxp://arbruisseau[.]com/profiles/db_template.php
hxxp://ladiescircle.co.za//db_template.php
hxxp://all-reseller[.]com/zzz_backup/db_template.php
hxxp://alcatrazmoon[.]com/images/db_template.php
hxxp://www.alcalumni[.]com/wp-includes/db_template.php
hxxp://aniljoseph[.]com/servermon/db_template.php
hxxp://alwake3press[.]com/wp-includes/db_template.php
hxxp://www.hfhl.org.ls/habitat/db_template.php
hxxp://alcafricanos[.]com/slsmonographs/db_template.php
hxxps://agapeencounter.org//db_template.php
hxxp://apobiomedix.ca//db_template.php
hxxp://anythinglah.info//db_template.php
hxxp://aniroleplay.net//db_template.php
hxxp://www.allcopytoners[.]com//db_template.php
hxxp://alphaobring[.]com//db_template.php
hxxp://www.galwayprimary.co.za//db_template.php
hxxp://alnuzha.org/en/db_template.php
hxxps://ancient-wisdoms[.]com//db_template.php
hxxp://amazingenergysavings.net//db_template.php
hxxp://gvs[.]com.pk/font-awesome/db_template.php
hxxp://geetransfers.co.za/font-awesome/db_template.php
hxxp://carlagrobler.co.za/components/db_template.php
hxxp://amazingashwini[.]com//db_template.php
hxxp://aminearserver.es//db_template.php
hxxp://lensofafrica.co.za//db_template.php
hxxp://greenacrestf.co.za/video/db_template.php
hxxp://www.tonaro.co.za//db_template.php
hxxp://alephit2.biz/kitzz/db_template.php
hxxp://lppaportal.org.ls//db_template.php
hxxp://alkousy[.]com//db_template.php
hxxp://ambulatorioveterinariocalusco[.]com/img/common/db_template.php
hxxp://fragranceoil.co.za//db_template.php
hxxp://www.eloquent.co.za/nweb2/db_template.php
hxxp://chrishanicdc.org/wpimages/db_template.php
hxxp://ahc.me.uk//db_template.php
hxxp://www.britishasia-equip.co.uk//db_template.php
hxxp://always-beauty.ch//db_template.php

hxxps://www.ancamamara[.]com/wp-admin/db_template.php
hxxp://entracorntrading.co.za//db_template.php
hxxp://www.alexjeffersonconsulting[.]com/wp-includes/db_template.php
hxxp://americabr[.]com.br//db_template.php
hxxp://andrew-snyder.net/bootstrap/db_template.php
hxxp://signsoftime.co.za//db_template.php
hxxp://aperta-armis.org//db_template.php
hxxp://absfinancialplanning.co.za/images/db_template.php
hxxp://charispaarl.co.za//db_template.php
hxxp://indlovusecurity.co.za//db_template.php
hxxp://alcafricandatalab[.]com//db_template.php
hxxp://amor-clubhotels[.]com//db_template.php
hxxp://mokorotlocorporate[.]com//db_template.php
hxxp://appppriori[.]com//db_template.php
hxxp://luxconprojects.co.za//db_template.php
hxxp://androidphonetips[.]com/wp-includes/db_template.php
hxxp://angel-seeds[.]com.ua/catalog/db_template.php
hxxp://alissanicolai[.]com/assets/db_template.php
hxxps://www.amateurastronomy.org//db_template.php
hxxp://aiofotoevideo[.]com//db_template.php
hxxp://www.amika.hr//db_template.php
hxxp://comfortex.co.za/php/db_template.php
hxxp://deepgraphics.co.za//db_template.php
hxxps://agiledepot[.]com//db_template.php
hxxp://almatours.gr//db_template.php
hxxp://analystcnwang[.]com//db_template.php
hxxp://www.malboer.co.za/trendy1/db_template.php
hxxp://sefikengfarm.co.ls//db_template.php
hxxp://www.antirughenaturale[.]com/wp-admin/db_template.php
hxxp://passright.co.za//db_template.php
hxxp://seismicfactory.co.za//db_template.php
hxxp://alessandroalessandrini.it//db_template.php
hxxps://aquabsafe[.]com//db_template.php
hxxp://amatikulutours[.]com/tmp/db_template.php
hxxp://ganitis.gr//db_template.php
hxxp://aleenasgiftbox[.]com/admin/db_template.php
hxxps://allusdoctors[.]com/themes/db_template.php
hxxp://alainsaffel[.]com//db_template.php
hxxp://www.ariehandomri[.]com//db_template.php
hxxp://aquaneeka.co.uk/wp-includes/db_template.php
hxxp://itengineering.co.za/gatewaydiamond/db_template.php
hxxp://alldomains-crm[.]com/bubblegumpopcorn[.]com/wp-admin/db_template.php

hxxp://www.albertamechanical.ca//db_template.php
hxxp://alchamel.info//db_template.php
hxxps://almokan.net/wp-includes/db_template.php
hxxp://jakobieducation.co.za//db_template.php
hxxps://arc-sec.net//db_template.php
hxxp://ldams.org.ls/supplies/db_template.php
hxxp://menaboracks.co.za/tmp/db_template.php
hxxp://www.getcord.co.za//db_template.php
hxxp://boardaffairs[.]com//db_template.php
hxxp://capetownway.co.za//db_template.php
hxxp://cloudhostdesign[.]com//db_template.php
hxxp://hartenboswaterpark.co.za/templates/db_template.php
hxxp://fccorp.co.za/php/db_template.php
hxxp://angar68[.]com//db_template.php
hxxp://www.dws-gov.co.za//db_template.php
hxxp://alwahahweb[.]com//db_template.php
hxxp://anuragcreatives[.]com//db_template.php
hxxp://embali.co.za//db_template.php
hxxp://albertaedmonton[.]com/widgetstyles/db_template.php
hxxp://altosdefontana[.]com//db_template.php
hxxp://airfanhydro.net//db_template.php
hxxps://www.alexponcet[.]com/wp-includes/db_template.php
hxxp://agropecuariavilarica[.]com.br//db_template.php
hxxps://www.amazingbuyrd[.]com/admin/db_template.php
hxxp://cdxtrading.co.za//db_template.php
hxxp://interafricaconsulting[.]com/wpimages/db_template.php
hxxp://glgroup.co.za/images/db_template.php
hxxp://hisandherskennels.co.za/php/db_template.php
hxxp://alemaohost[.]com/lotosorg[.]com/db_template.php
hxxp://isibaniedu.co.za/admin/db_template.php
hxxp://dianakleyn.co.za/layouts/db_template.php
hxxp://themotoringcalendar.co.za//db_template.php
hxxp://www.loansonhomes.co.za//db_template.php
hxxp://edgesecurity.co.za/js/db_template.php
hxxp://highschoolsuperstar.co.za/files/db_template.php
hxxp://www.ambientproperty[.]com//db_template.php
hxxp://animationshowreel.co.il//db_template.php
hxxp://cafawelding.co.za/font-awesome/db_template.php
hxxp://apalawyers.pt//db_template.php
hxxp://www.edesignz.co.za//db_template.php
hxxp://centuryacademy.co.za/css/db_template.php
hxxps://ambyenta.hr//db_template.php

hxxp://ceramica.co.za//db_template.php
hxxp://www.alfredoposada[.]com//db_template.php
hxxp://anastasovsworkshop[.]com/wp-includes/db_template.php
hxxp://allisonplumbing[.]com/wp-includes/db_template.php
hxxp://eastrandmotorlab.co.za/fleet/db_template.php
hxxp://angelsongroup[.]com/wp-includes/db_template.php
hxxp://www.mikimaths[.]com//db_template.php
hxxp://hjb-racing.co.za/htdocs/db_template.php
hxxp://anotherpartofme[.]com/wp-includes/db_template.php
hxxp://www.andreabelfi[.]com//db_template.php
hxxp://www.iancullen.co.za//db_template.php
hxxp://alaskamaterials[.]com//db_template.php
hxxp://jeanetteproperties.co.za//db_template.php
hxxp://www.digitalmedia.co.za//db_template.php
hxxp://www.rejoicetheatre[.]com//db_template.php
hxxps://alterwebhost[.]com//db_template.php
hxxp://bc-u.co.uk//db_template.php
hxxp://dpscdgkhan.edu.pk/shopping/db_template.php
hxxp://edgeforensic.co.za//db_template.php
hxxp://willpowerpos.co.za//db_template.php
hxxp://antrismode[.]com/wp-includes/db_template.php
hxxp://colenesphotography.co.za/modules/db_template.php
hxxp://anthaigroup.vn//db_template.php
hxxps://alphainvestors[.]com.au//db_template.php
hxxps://aliart.nl//db_template.php
hxxps://allmantravel[.]com/thumbs/db_template.php
hxxp://fbrvolume.co.za//db_template.php
hxxp://amordegato.es/storefront/db_template.php
hxxp://agylub[.]com//db_template.php
hxxp://www.khotsonglodge.co.ls//db_template.php
hxxp://ampli5yd[.]com//db_template.php
hxxps://animeok.co.il//db_template.php
hxxps://arbeidsrechtcentrum.nl//db_template.php
hxxp://erniecommunications.co.za/js/db_template.php
hxxp://promechtransport.co.za/scripts/db_template.php
hxxp://centuriongsd.co.za//db_template.php
hxxp://www.agencesylvieleclerc[.]com//db_template.php
hxxp://delcom.co.za//db_template.php
hxxps://aleoestudio[.]com/gallonature/db_template.php
hxxp://oftheearthphotography[.]com/www/db_template.php
hxxp://h-dubepromotions.co.za//db_template.php
hxxp://www.alessioborzuola[.]com/downloads/db_template.php

hxxp://crystaltidings.co.za//db_template.php
hxxp://funeralbusinesssolution[.]com/email_template/db_template.php
hxxp://funisalodge.co.za/data1/db_template.php
hxxp://experttutors.co.za//db_template.php
hxxps://www.cartridgecave.co.za//db_template.php
hxxp://ecs-consult[.]com//db_template.php
hxxp://www.animationinisrael.org/tmp_images/db_template.php
hxxp://gideonitesprojects[.]com//db_template.php
hxxp://hybridauto.co.za/photography/db_template.php
hxxp://africanpixels.zar.cc//db_template.php
hxxp://ryanchristiefurniture.co.za//db_template.php
hxxp://evansmokaba[.]com/evansmokaba[.]com/thabiso/db_template.php
hxxp://almeriahotelja[.]com/dk/db_template.php
hxxp://al3abflash.biz//db_template.php
hxxp://www.fun4kidz.co.za//db_template.php
hxxp://alsharhanstore[.]com//db_template.php
hxxp://www.infratechconsulting[.]com//db_template.php
hxxp://algihad[.]com/assets/db_template.php
hxxp://americanwestmedia[.]com//db_template.php
hxxp://charliewestsecurity.co.za//db_template.php
hxxp://beehiveholdingszar.co.za//db_template.php
hxxp://analyticalfootball[.]com//db_template.php
hxxp://apiiination[.]com/leadership/db_template.php
hxxps://ahelicoptermom[.]com/wp-includes/db_template.php
hxxp://servicebox.co.za//db_template.php
hxxp://globalelectricalandconstruction.co.za/wpscripts/db_template.php
hxxps://aquo.in//db_template.php
hxxps://www.alfransia[.]com/wp-admin/db_template.php
hxxp://www.icsswaziland[.]com//db_template.php
hxxp://aiko.pro//db_template.php
hxxps://alceharfield[.]com//db_template.php
hxxp://indocraft.co.za/test/db_template.php
hxxp://allegiancesecurity.org//db_template.php
hxxp://sullivanprimary.co.za//db_template.php
hxxp://www.apmequestrian[.]com//db_template.php
hxxps://alphawaves.org/wp-admin/db_template.php
hxxp://www.alexandrasternin[.]com/illustration/db_template.php
hxxp://www.daleth.co.za//db_template.php
hxxp://jwseshowe.co.za/assets/db_template.php
hxxp://winagainstebola[.]com//db_template.php
hxxp://anubandh.in//db_template.php
hxxp://www.alexanderhomestead[.]com//db_template.php

hxxp://alfatek-intelligence[.]com//db_template.php
hxxp://www.aprendiendoencasa[.]com/wp-includes/db_template.php
hxxp://alorabrownies[.]com/wp-admin/db_template.php
hxxp://andrasadam[.]com/tothildiko/wp-includes/db_template.php
hxxp://cazochem.co.za/cazochem/db_template.php
hxxp://debnoch[.]com/image/db_template.php
hxxp://hmholdings360.co.za//db_template.php
hxxp://iinvest4u.co.za//db_template.php
hxxp://burgercoetzeeattorneys.co.za//db_template.php
hxxp://anngrigphoto[.]com//db_template.php
hxxp://alchemistasonida[.]com//db_template.php
hxxp://anahera.biz/admin/db_template.php
hxxp://h-u-i.co.za/heiren/db_template.php
hxxp://insta-art.co.za//db_template.php
hxxp://muallematsela[.]com//db_template.php
hxxp://aguasdecastilla[.]com/uploads/db_template.php
hxxp://www.arabgamenetwork[.]com//db_template.php
hxxps://arhiepiscopiabucurestilor.ro/templates/db_template.php
hxxp://amruthavana[.]com/blog/db_template.php
hxxp://digitalblue.co.za//db_template.php
hxxps://www.alvarezarquitectos[.]com//db_template.php
hxxp://buboobioinnovations.co.za/wpimages/db_template.php
hxxp://andrewsbisom[.]com//db_template.php
hxxp://www.m-3.co.za//db_template.php
hxxp://beesrenovations.co.za/images/db_template.php
hxxps://www.apliety.co.il/wp-includes/db_template.php
hxxp://alchamelup.org/htdocs/db_template.php
hxxp://benonicoc.co.za/resources/db_template.php
hxxps://al-mostakbl[.]com//db_template.php
hxxp://alchimiegrafiche.net/bbdelteatro/db_template.php
hxxp://andrespazsoldan[.]com//db_template.php
hxxp://in2accounting.co.za//db_template.php
hxxp://aipa.ca//db_template.php
hxxp://alphabee.fund/PHPMailer_5.2.0/db_template.php
hxxp://arabsdeals[.]com//db_template.php
hxxps://archiotronic[.]com/wp-includes/db_template.php
hxxp://capewindstrading.co.za//db_template.php
hxxps://althurayaa[.]com//db_template.php
hxxp://jhphotoedits.co.za//db_template.php
hxxp://cloudhub.co.ls/modules/db_template.php
hxxp://apironco[.]com/wp-includes/db_template.php
hxxp://digital-cameras-south-africa.co.za/script/db_template.php

hxxp://ahmadhasanat[.]com//db_template.php
hxxp://alexrocchi[.]com//db_template.php
hxxp://aljaadi[.]com//db_template.php
hxxps://www.engeltjieakademie.co.za//db_template.php
hxxp://annabelle.nl/next/db_template.php
hxxp://juniorad.co.za/vendor/db_template.php
hxxp://animationpulse.net//db_template.php
hxxp://angloglot[.]com//db_template.php
hxxp://agricolavicuna.cl//db_template.php
hxxp://alexelgy[.]com/allaccess/db_template.php
hxxp://www.centreforgovernance.uk//db_template.php
hxxp://www.aliandconsulting[.]com//db_template.php
hxxp://balaateen.co.za/less/db_template.php
hxxp://aleksicdunja[.]com//db_template.php
hxxp://arestihome[.]com//db_template.php
hxxp://am1int.fcomet[.]com/wp1/db_template.php
hxxp://anet-international-group[.]com/shop/db_template.php
hxxp://courtesydriving.co.za/js/db_template.php
hxxp://annaplebanek[.]com//db_template.php
hxxp://agencijazemil[.]com//db_template.php
hxxp://airminumtiro[.]com//db_template.php
hxxp://www.androidwikihow[.]com//db_template.php
hxxp://alisabyfinna[.]com//db_template.php
hxxp://rma-law.co.za//db_template.php
hxxp://amari.ro/components/db_template.php
hxxp://anxiousandunstoppable[.]com//db_template.php
hxxp://www.buhlebayoacademy[.]com//db_template.php
hxxp://arabellajo[.]com/wp/wp-includes/db_template.php
hxxp://blackthorn.co.za//db_template.php
hxxp://alaqaba[.]com/dnsarabia[.]com/db_template.php
hxxp://airesis.blog/wp-admin/db_template.php
hxxp://www.aptibet.org//db_template.php
hxxp://alecattic[.]com/wp-includes/db_template.php
hxxp://anglero[.]com//db_template.php
hxxp://getabletravel.co.za/wpscripts/db_template.php
hxxp://www.allwestdental[.]com/wp-includes/db_template.php
hxxp://printernet.co.za//db_template.php
hxxp://genesisbs.co.za//db_template.php
hxxp://allsporthealthandfitness[.]com//db_template.php
hxxp://www.humorcarbons[.]com//db_template.php
hxxp://intelligentprotection.co.za//db_template.php
hxxp://amazethings[.]com//db_template.php

hxxp://incoso.co.za/images/db_template.php
hxxp://www.antoanetapalikarska[.]com//db_template.php
hxxps://www.alteaparadise[.]com/wp-includes/db_template.php
hxxp://amirmenahem[.]com//db_template.php
hxxp://isound.co.za//db_template.php
hxxp://www.alestilorachel[.]com//db_template.php
hxxp://alcfm.net/wp-admin/db_template.php
hxxp://www.acer-parts.co.za//db_template.php
hxxp://www.gsmmid[.]com//db_template.php
hxxp://skhaleni.co.za//db_template.php
hxxps://amiici.vision//db_template.php
hxxps://andihaas.at/wp-includes/db_template.php
hxxp://www.albertaprimebeef[.]com//db_template.php
hxxps://www.appster.it/wp-includes/db_template.php
hxxp://amofoundation.org/wp-includes/db_template.php
hxxp://iqra.co.za/pub/db_template.php
hxxp://thecompasssolutions.co.za//db_template.php
hxxp://archwaycarpetscrm.co.uk//db_template.php
hxxp://iggleconsulting[.]com//db_template.php
hxxps://angel-blanco.net/wp-includes/db_template.php
hxxps://anotherdayinparadise.ca//db_template.php
hxxp://www.bitp.co.za//db_template.php
hxxp://cupboardcure.co.za/vendor/db_template.php
hxxp://all2wedding[.]com/wp-includes/db_template.php
hxxp://allianz[.]com.pe/wp-admin/db_template.php
hxxp://amiehepperlin[.]com//db_template.php
hxxps://www.amighini.it/webservice/db_template.php
hxxp://broken-arrow.co.za//db_template.php
hxxp://www.ihlosiqs-pm.co.za//db_template.php
hxxp://alisimple.si/wp-includes/db_template.php
hxxp://allthat.social//db_template.php
hxxp://www.amphibiblechurch[.]com//db_template.php
hxxp://bestencouragementwords[.]com//db_template.php
hxxp://alayhamtechnologies[.]com//db_template.php
hxxps://alaskanharvestseafood[.]com/backup/db_template.php
hxxps://www.air-mag.ro//db_template.php
hxxp://get-paid-for-online-survey[.]com//db_template.php
hxxp://www.antc.ch/wp-includes/db_template.php
hxxp://firstchoiceproperties.co.za//db_template.php
hxxp://habibtextiles.pk//db_template.php
hxxp://fsproperties.co.za/engine1/db_template.php
hxxp://diegemmerkat.co.za//db_template.php

hxxp://molepetravel.co.ls//db_template.php
hxxp://mmetl.co.za//db_template.php
hxxp://altrablog[.]com//db_template.php
hxxp://abrahamseed.co.za//db_template.php
hxxp://www.amerindgen[.]com/author/admin1/db_template.php
hxxp://altcoinaddict[.]com//db_template.php
hxxp://iiee.edu.pk//db_template.php
hxxp://cmhts.co.za/resources/db_template.php
hxxp://domesticguardians.co.za/Banner/db_template.php
hxxps://amishcountryfurnishings[.]com//db_template.php
hxxps://allday.gr//db_template.php
hxxp://www.alinn-u-yin[.]com//db_template.php
hxxps://www.allin-chain[.]com//db_template.php
hxxps://www.anatapackaging[.]com/vendors/db_template.php
hxxp://alexcelts[.]com/wp/db_template.php
hxxp://www.allstylus[.]com.br//db_template.php
hxxp://www.algom-law[.]com//db_template.php
hxxp://ambiances-toiles.fr//db_template.php

Popular posts from this blog

[POWERSING - FROM LNK FILES TO JANICAB THROUGH YOUTUBE & TWITTER]

INTRODUCTION This post will discuss an ongoing campaign that have been operational since at least August 2017 . The post will look into the delivery of the malware, some analysis on the payload, and some additional insights in relation to the campaign. It is by no means a full in depth analysis of the malware and all it's functionality. LAWYER UP!! This all started with a tweet by the AWESOME Jacob Soo (@_jsoo_) whom I recommend you go and follow if you are interested in analyzing malware and tracking different threat actors. The sample is a ZIP file titled "Dubai_Lawyers_update_2018.zip" and the archive contains two LNK files that are perpetrating to be PDF files. The actors in this case borrowed couple of files from the British Embassy site and used them as decoy documents to lure victims into believing that these files are in fact legitimate. https://assets.publishing.service[.]gov.uk/government/uploads/system/uploads/attachment_da...

[HOW DO YOU LIKE DEM EGGS? I LIKE MINE SCRAMBLED, REALLY SCRAMBELED - A LOOK AT A RECENT more_eggs SAMPLES]

BACKGROUND The topic of discussion have been covered quite well in the past years. With some analysis focusing on the human element and actors behind the tools and other analysis attributing to different groups and some focusing on the malware and final payload . This blog will just focus on some recent samples related to what i think is more_eggs and my attempt (successful or not, I will let you be the judge of that) at analyzing them and some questions I have. I won't be discussing any attribution or provide my thoughts on that in this blog. HIGH LEVEL ANALYSIS OF SAMPLES This all started with a tweet - https://twitter.com/jaydinbas/status/1633063201607675909?s=20 File Name : Axiance_Full_Reports[.]zip Hash : 631f92c9147733acf3faa02586cd2a6cda673ec83c24252fccda1982cf3e96f6 The file is a ZIP file that include an LNK file and a JPG. The LNK as you would expect includes an obfuscated code within it that is consis...
