

# Burping on MuddyWater

[sec0wn.blogspot.com/2018/02/burping-on-muddywater.html](https://sec0wn.blogspot.com/2018/02/burping-on-muddywater.html)

Mo Bustami

## INTRODUCTION

In an earlier [blog posts](#), I wrote about a campaign that was targeting the Middle East (Saudi Arabia, Iraq, UAE, etc). The adversary group behind this campaign was covered by PaloAlto's [UNIT42](#) and [others](#) under the name MuddyWater.

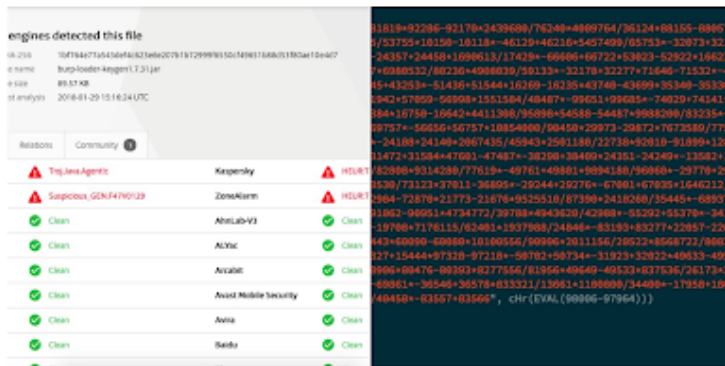
In this blog I will be sharing new samples related to this adversary group and how they are continuing to evolve and how they shifted some of their delivery tactics.

## IT ALL STARTS WITH A TWEET.

This all started when I saw a [tweet](#) from [@x0rz](#) referring to a [blogpost](#) where they reversed a BurpSuite Key Generator.



Reversing a Burp Keygen (burp-loader-keygen1.7.31.jar), guess what? It's #malware [0x00sec.org/t/malware-reve...](https://0x00sec.org/t/malware-reve...) #reverseengineering



12:37 PM - 30 Jan 2018

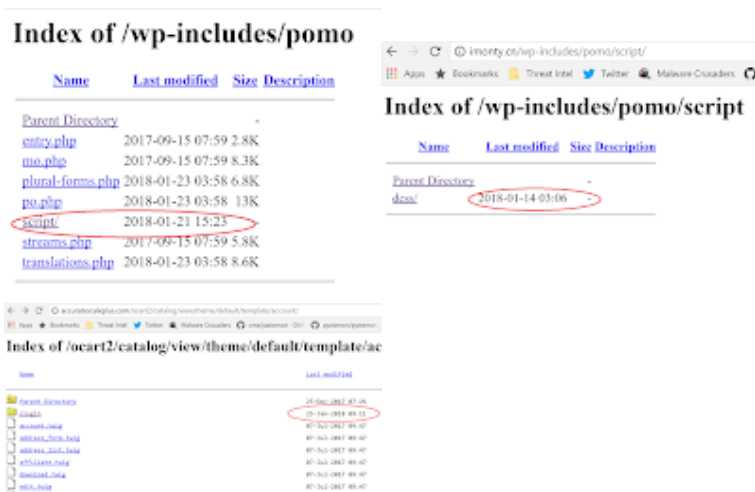
I recommend everyone to go and read the above mentioned blogpost as it is really well done and goes into detail regarding the analysis of this malicious Key Generator. I will NOT be covering the analysis again since the folks at [0x00sec](#) covered it amazingly.

I will be providing some additional IoCs related to this campaign, discuss the shift in the techniques used by MuddyWater and cast a few questions that are surrounding this actor.

But first lets explain couple of terms:



- '无法连接到网址，请等待龙...' which google translate to 'Can not connect to website, please wait for dragon ...' - Interestingly enough, the variable that holds the different proxy sites is called "{dRaGoN\_MlDdLe}"
- "无法访问本地计算机寄存器" which google translate to "Can not access local computer register"
- "任务计划程序访问被拒绝" which google translate to "Task Scheduler Access Denied" - As you can see the last two are related to the persistence of the malware in the victim's machine.
- **Timeline** - I was able to find another earlier [sample "dfd796b35260de18bd1ed9e31c33520e"](#) using the same type of delivery as in Trojanized KeyGen. This could mean that this campaign has been ongoing since at least end of December. Additionally, quick look at the domains where the initial scripts were hosted, it seems like the malicious scripts have been removed as of the writing of this blog since the domains had open directories showing last modified dates as below



## FINAL THOUGHTS

This shows that MuddyWater group is continuing activity and might be looking to change some of their techniques. However, this just creates more questions than answers and add to the great reason behind naming them MuddyWater.

1. **Why the Change in delivery mechanism?** This can be easily to evade existing detection and looking at other ways rather than just weaponized documents.
2. **Are they changing their targeting?** BurpSuite is mainly used by either Web Application Security researchers or other attackers and hackers. Is MuddyWater trying to compromise other attacker groups or are they after security researchers?
3. **How deep does the Rabbit Hole goes??** I was able to just come across the two samples mentioned. There are probably more. They even might have also trojanized other tools. Or even experimenting with other delivery mechanism.

Below you will find a list of IoCs from my analysis and I am sure other will be able to dig deeper into this an uncover further details. Hope this is of help and benefit.

## INDICATORS OF COMPROMISE

## HASHES

---

5db9cd9f1dd2bc0e183786f587c1e1ac93097a0ab6d258d0f3dc846e621c881f  
81ea842f0579a1d55a31eca17f06f438f1e52d687ef2de4af97adbe9b6d29571  
00a5fc1122b1a219ce92ea65c7c6d89f3133f60457e08546380a562b0ee7fbdf  
3849d62dfffb2745c6bc9cb6a128f9ede9136a3979ee3ff7b498057e51ddd25c9  
1bf764e77a543def4c623e6e207b1b72999f6550cf49651b88d53f80ae10e4d7  
ddc65d70b001baeea348c906e21219a49dda64f32c8f6732a56491620bdf7bf4  
36754180d3d036fba9c6f5cfec12a8fb7a90d10ef37d99c05c0782fbb49dcce  
ffc0520d2f3651ed4e04c737d92d8398d680b468937765705c92e16ac41d5aa6  
dc64abcefd9250c3db4b9de90d2b307aa2dc9e4b998c46899bd1a6e837fa5180  
34147db3241ca1f7f14ae7efb44658dcc92c0e7822e949380165d906340a9158  
a16645aa0f879a874605db8380c06e19ba68ddbdd2af8e54577a6334e0d2f3c2

## DOMAINS & URLs

---

**SAMPLE** - hxxp://www[.]hackingcrunch.com/wp-content/uploads/Burp/burpsuite\_pro\_v1.7.30.zip

## PROXY LIST

---

hxxp://aandacompany[.]com/connection[.]php  
hxxp://ankara24saatacickicekci[.]com/admin/connection[.]php  
hxxp://ankara24saatcicek[.]com/admin/controller/common/connection[.]php  
hxxp://ankara24saatcicek[.]net/admin/controller/play/connection[.]php  
hxxp://ankaraikincielesyalar[.]com/admin/\_sayfalar/connection[.]php  
hxxp://ankarakiralikvinc[.]web[.]tr/wp-admin/connection[.]php  
hxxp://ankaramehteri[.]com/admin/\_islemler/connection[.]php  
hxxp://ankaraotokurtarici[.]web[.]tr/wp-includes/connection[.]php  
hxxp://aazbs[.]com/wp-admin/includes/connection[.]php  
hxxp://ankaratemizlik[.]web[.]tr/include/connection[.]php  
hxxp://ankaratemizlikirsirketleri[.]web[.]tr/wp-includes/connection[.]php  
hxxp://www[.]aofdersleri[.]net/wp-admin/connection[.]php  
hxxp://www[.]aofdersleri[.]net/wp-content/themes/hueman/connection[.]php  
hxxp://apaktem[.]com/wp-admin/connection[.]php  
hxxp://aquamasaj[.]com/ozzzpanel/documentation/connection[.]php  
hxxp://aracexpress[.]com/wp-admin/connection[.]php  
hxxp://arasbg[.]com/yonetimpaneli/connection[.]php  
hxxp://ardatur[.]com/sayfalar/connection[.]php  
hxxp://ardvessels[.]com/online-catalog/connection[.]php  
hxxp://artikhazirsin[.]remingtonturkiye[.]com/erkek/wp-admin/sconnection[.]php  
hxxp://artistanbul[.]tv/wp-admin/connection[.]php  
hxxp://artistlogistics[.]net/wp-admin/connection[.]php  
hxxp://artistlogistics[.]net/wp-includes/connection[.]php  
hxxp://aslanmangalkomuru[.]com/panel/connection[.]php  
hxxp://aslanorganizasyon[.]com//fonts/icomoon/connection[.]php  
hxxp://aslimaj[.]com/wp-admin/connection[.]php

hxxp://astra[.]com[.]tr/master/sass/vendor/bourbon/helpers/connection[.]php  
hxxp://asturkgrup[.]com/ar/cache/connection[.]php  
hxxp://asturkgrup[.]com/ar/yonetimpaneli/connection[.]php  
hxxp://asturkkimya[.]com/W3/fonksiyon/connection[.]php  
hxxp://asturkmadencilik[.]com/inc/connection[.]php  
hxxp://atakantarimci[.]com[.]tr/wp-admin/connection[.]php  
hxxp://ataklojistik[.]com/administrator/modules/mod\_toolbar/connection[.]php  
hxxp://atamanelektronik[.]com/administrator/components/com\_banners/connection[.]php  
hxxp://atamanelektronik[.]com/components/com\_content/models/connection[.]php  
hxxp://atasehiryuzme[.]com/wp-admin/connection[.]php  
hxxp://atasehiryuzme[.]com/wp-includes/Requests/connection[.]php  
hxxps://www[.]atayuzme[.]com[.]tr/deneme1/connection[.]php  
hxxp://atkiatkisi[.]net/panel/connection[.]php  
hxxp://atkiatkisiimalat[.]com//blog/wp-admin/connection[.]php  
hxxp://avrupabaski[.]com/yillik/cmsal2017/connection[.]php  
hxxp://avsserradecor[.]com/katalog/mobile/styles/connection[.]php  
hxxp://ayakkabisitesi[.]com/wp-admin/connection[.]php  
hxxp://aycinteker[.]com/wp-admin/connection[.]php  
hxxp://aydincaliskankanarya[.]com/wp-admin/connection[.]php  
hxxp://aydincaliskankanarya[.]com/wp-content/themes/twentyseventeen/connection[.]php  
hxxp://aydinsenturk[.]com/ozerkaya/connection[.]php  
hxxp://aygunotomasyon[.]com/administrator/components/com\_languages/connection[.]php  
hxxp://aygunotomasyon[.]com/components/com\_user/connection[.]php  
hxxp://aymuhendislik[.]com/wp-admin/connection[.]php  
hxxp://aymuhendislik[.]com/wp-includes/ID3/connection[.]php  
hxxp://aysekaya[.]com[.]tr/wp-admin/connection[.]php  
hxxp://azermaral[.]com/wp-admin/connection[.]php  
hxxp://bahadirsahinoglu[.]com/wp-admin/connection[.]php  
hxxp://bahadirsahinoglu[.]com/wp-includes/connection[.]php  
hxxp://baharakgul[.]com/wp-admin/connection[.]php  
hxxp://balcidede[.]com[.]tr/admin/inc/connection[.]php  
hxxp://baldatca[.]com/admin/controller/extension/connection[.]php  
hxxp://baldatca[.]com/system/config/connection[.]php  
hxxp://baranakinturk[.]com[.]tr/wp-includes/ID3/connection[.]php  
hxxp://baskale[.]bel[.]tr/admin/inc/connection[.]php  
hxxp://baskoyluhasanefendi[.]com/administrator/includes/connection[.]php  
hxxp://baspinarlartulumpeyniri[.]com/wp-admin/connection[.]php  
hxxp://bayrampasabocekilaclama[.]net/wp-content/plugins/google-sitemap-generator/connection[.]php  
hxxp://bebekyuzmekurslari[.]com/wp-admin/connection[.]php  
hxxp://bebekyuzmekurslari[.]com/wp-admin/connection[.]php  
hxxp://www[.]berkyilmaz[.]com[.]tr/wp-admin/connection[.]php  
hxxp://bervin[.]com[.]tr/yonetimpaneli/fonksiyonlar/connection[.]php  
hxxp://beyazavukatlik[.]com/wp-admin/connection[.]php

hxxp://beyzbolturk[.]com/wp-admin/includes/connection[.]php  
hxxp://bienart[.]com/cagdaz/panel/connection[.]php  
hxxp://bifikirajans[.]com/hosting2/connection[.]php  
hxxp://bihaliortusu[.]com/wp-content/plugins/js\_composer/config/deprecated/connection[.]php  
hxxp://bilenbizibilir[.]com/wp-includes/connection[.]php  
hxxp://bilsem[.]club/forum/connection[.]php  
hxxp://biodogacevre[.]com/admin/css/connection[.]php  
hxxp://birfidanbirumut[.]org[.]tr/admin/ckeditor/connection[.]php  
hxxp://bitekservis[.]com/adamsin/controller/sale/connection[.]php  
hxxp://bitekservis[.]com/adamsin/model/sample/lexus\_superstore/connection[.]php  
hxxp://biyanyapi[.]com/deneme/connection[.]php  
hxxp://bmenerji[.]com[.]tr/wp-admin/connection[.]php  
hxxp://bmenerji[.]com[.]tr/wp-includes/connection[.]php  
hxxp://bocekilaclama[.]gen[.]tr/admin/connection[.]php  
hxxp://bocekilaclamahizmeti[.]com/wp-admin/connection[.]php  
hxxp://bocekilaclamazeytinburnu[.]net/wp-includes/connection[.]php  
hxxp://bolgemuhabirligi[.]com/wp-admin/connection[.]php  
hxxp://booksandtoys[.]com[.]tr/admin/controller/design/connection[.]php  
hxxp://bor[.]superyaz[.]com/admin/controller/catalog/connection[.]php  
hxxp://brctsrn[.]com/wp-admin/connection[.]php  
hxxp://bsmtrans[.]com/eskiindex-php/\_modules/connection[.]php  
hxxp://btafbearings[.]com/connection[.]php  
hxxp://burakdoseme[.]com/admin/ckeditor/connection[.]php  
hxxp://burkertparts[.]com/include/connection[.]php  
hxxp://www[.]aalotv[.]com/wp-admin/connection[.]php  
hxxp://acmecepl[.]com/connection[.]php  
hxxps://aareezenterprises[.]com/php/connection[.]php  
hxxp://laserswat[.]com/admin/language/english/payment/connection[.]php  
hxxp://ksu[.]com[.]tr/admin53x/ckfinder/core/connector/php/lang/connection[.]php  
hxxp://www[.]lamiademir[.]com/myadmin/connection[.]php  
hxxp://admissions[.]ae/wp-content/upgrade/connection[.]php  
hxxp://liladecor[.]com[.]tr/administrator/templates/system/connection[.]php  
hxxp://agripal[.]ae/wp/wp-includes/IXR/connection[.]php  
hxxp://kuzeyyeliinsaati[.]com[.]tr/admin/connection[.]php  
hxxp://www[.]ajmansexymassagebodytobody[.]com/js/connection[.]php  
hxxp://krediogren[.]net/wp-content/themes/TJG-magazine/connection[.]php  
hxxp://alarabtents[.]com/connection[.]php  
hxxp://aleter[.]ae/connection[.]php  
hxxp://alfahadmedia[.]ae/wp1/connection[.]php  
hxxp://limanyapidenetim[.]com[.]tr/admin/connection[.]php  
hxxp://www[.]alothman-gt[.]com/wp-includes/pomo/connection[.]php  
hxxp://azracateringme[.]ae/connection[.]php  
hxxp://bakemartplus[.]ae/bakemart[.]ae/connection[.]php  
hxxp://www[.]agrininmarkalari[.]com/wp-content/themes/tema/connection[.]php

hxxp://bhic-group[.]com/wp-includes/images/smilies/connection[.]php  
hxxp://www[.]big-bang[.]ae/wp-content/themes/twentyfifteen/genericons/connection[.]php  
hxxp://bloorco[.]com/vendor/jquery/connection[.]php  
hxxp://aitech[.]com[.]tr/admin/connection[.]php  
hxxp://bwtest1[.]apps[.]ae/wp-includes/pomo/connection[.]php  
hxxp://capital[.]wistech[.]biz/wp-includes/customize/connection[.]php  
hxxp://akademihastanesi[.]net/wp-content/themes/twentyseventeen/connection[.]php  
hxxp://www[.]akkurtgida[.]com[.]tr/tr/templates/atomic/connection[.]php  
hxxp://chat[.]honda[.]ae/support/html/connection[.]php  
hxxp://www[.]clearviewuae[.]com/wp-includes/widgets/connection[.]php  
hxxp://cmsolutions[.]ae/wp-includes/fonts/connection[.]php  
hxxp://cool-group[.]net/pm/connection[.]php  
hxxp://mistcool[.]ae/connection[.]php  
hxxp://bigfans[.]ae/connection[.]php  
hxxp://cool-group[.]net/support/connection[.]php  
hxxp://cooldoctor[.]ae/less/connection[.]php  
hxxp://akparplastik[.]com/connection[.]php  
hxxp://coolingdubai[.]com/connection[.]php  
hxxp://mistingdubai[.]net/connection[.]php  
hxxp://aysamturizm[.]com[.]tr/wp-includes/connection[.]php  
hxxp://azizinsaat[.]com/panelim/connection[.]php  
hxxp://aypir[.]com/wp-admin/connection[.]php  
hxxp://delinmeal[.]com/inventory/connection[.]php  
hxxp://www[.]basoglucit[.]com/wp-includes/theme-compat/connection[.]php  
hxxp://bckkaucuk[.]com/wp-admin/connection[.]php  
hxxp://davetyaymak[.]com/sys/connection[.]php  
hxxp://dikon[.]com[.]tr/connection[.]php  
hxxp://drhalilciftci[.]com/cache/connection[.]php  
hxxps://dubailegaleagle[.]com/wp-includes/customize/connection[.]php  
hxxp://dubaistars[.]ae/engine1/connection[.]php  
hxxp://elitecaptains[.]ae/wp-includes/ID3/connection[.]php  
hxxp://egzotikshop[.]com/connection[.]php  
hxxp://ekrembahcekapili[.]com/vendor/composer/connection[.]php  
hxxp://erzincansrc[.]com/site/connection[.]php  
hxxp://www[.]gokhanturizmvetemizlik[.]com/wp-includes/connection[.]php  
hxxp://fitmentfurniture[.]com/wp-includes/certificates/connection[.]php  
hxxp://ftu965[.]com/wp-includes/theme-compat/connection[.]php  
hxxp://www[.]fullcircle-design[.]com/wp-includes/fonts/connection[.]php  
hxxps://galinusphysio[.]ae/connection[.]php  
hxxp://gulenapart[.]com/style/connection[.]php  
hxxp://ilaydapromosyon[.]com/components/com\_content/connection[.]php  
hxxp://cittaslowturkiye[.]org/wp-admin/user/connection[.]php  
hxxp://cuneytugur[.]com[.]tr/language/connection[.]php  
hxxp://drhalilciftci[.]com/connection[.]php





hxxp://www[.]il/wp-includes/widgets/connection[.]php  
hxxps://plush-toys[.]co[.]il/wp-includes/widgets/connection[.]php  
hxxp://yosifiko[.]co[.]il/wp-includes/widgets/connection[.]php  
hxxp://palmon-law[.]co[.]il/wp-includes/widgets/connection[.]php  
hxxp://www[.]mcb-law[.]co[.]il/wp-includes/widgets/connection[.]php  
hxxp://smart-sense[.]co[.]il/wp-includes/widgets/connection[.]php  
hxxp://azim[.]co[.]il/wp-includes/widgets/connection[.]php  
hxxps://dynamictours[.]co[.]il/components/connection[.]php  
hxxps://zahraty[.]com[.]sa/up/pub/media/yourstore/css/connection[.]php  
hxxps://www[.]wasa6h[.]com[.]sa/ws-admin/wy/skins/connection[.]php  
hxxps://www[.]wasa6h[.]com[.]sa/livezilla/images/geo/connection[.]php  
hxxps://jaras[.]sa/wp-includes/widgets/connection[.]php  
hxxps://zahraty[.]com[.]sa/up/app/design/frontend/connection[.]php  
hxxps://zahraty[.]com[.]sa/up/pub/media/yourstore/css/connection[.]php  
hxxps://tge[.]sa/tgefs/includes/js/bootstrap/connection[.]php  
hxxps://emobe[.]eu/wp-includes/widgets/connection[.]php  
hxxp://vlgstal[.]ru/wp-includes/widgets/connection[.]php  
hxxps://richmen[.]az/upgrades/connection[.]php  
hxxp://bg[.]com[.]tr/j3/components/com\_ajax/connection[.]php  
hxxp://www[.]rjsoftware[.]com/wp-content/themes/twentyseventeen/assets/css/connection[.]php  
hxxps://www[.]freesteamwalletcode[.]com/wp-content/languages/connection[.]php  
hxxps://www[.]icycheats[.]com/wp-includes/widgets/connection[.]php  
hxxp://mycar[.]ge/prava/jplot/docs/files/plugins/connection[.]php  
hxxps://goyalsoftech[.]com/css/imports/shortcodes/connection[.]php  
hxxps://pushconsole[.]com/assets/fonts/icomoon/connection[.]php  
hxxps://www[.]easykeysoftware[.]com/media/image/00/0d/9a/connection[.]php  
hxxp://mepure[.]com/connection[.]php  
hxxps://www[.]1n2r[.]com//wp-content/connection[.]php  
hxxps://www[.]1n2r[.]com//wp-content/themes/twenty-sixteen/inc/connection[.]php  
hxxp://bek[.]ae/wp-includes//connection[.]php  
hxxp://bek[.]ae/wp-includes//IXR/connection[.]php?lib=curl  
hxxps://climateplus[.]ae/wp-content/themes/tyche/connection[.]php  
hxxps://climateplus[.]ae/wp-content/themes/tyche/woocommerce/connection[.]php  
hxxp://lohuis[.]ae/wp-includes/widgets/connection[.]php  
hxxp://lohuis[.]ae/wp-includes/random\_compat/connection[.]php  
hxxps://mistingfan[.]ae/wp-content/themes/twenty-five/connection[.]php  
hxxps://mistingfan[.]ae/wp-content/themes/mts\_schema//connection[.]php  
hxxps://outdoorac[.]ae/wp-includes/ID3/connection[.]php  
hxxps://outdoorac[.]ae/wp-includes/customize/connection[.]php  
hxxps://outdoorcooling[.]ae/wp-includes/ID3/connection[.]php  
hxxps://outdoorcooling[.]ae/wp-includes/Text/connection[.]php  
hxxp://patioheater[.]ae/wp-content/plugins/connection[.]php  
hxxp://patioheater[.]ae/wp-includes/connection[.]php  
hxxps://hvls[.]ae/wp-includes/SimplePie/connection[.]php

hxxps://hvls[.]ae/wp-includes/SimplePie/Parse/connection[.]php  
hxxp://cool-group[.]ae/wp-includes/customize/connection[.]php  
hxxp://cool-group[.]ae/wp-includes/certificates/connection[.]php  
hxxp://adambaluch[.]ae/wp-includes/pomo/connection[.]php  
hxxp://adambaluch[.]ae/wp-includes/customize/connection[.]php  
hxxp://beachroad[.]ae/wp-includes/connection[.]php  
hxxp://beachroad[.]ae/wp-includes/Requests/Utility/connection[.]php  
hxxp://castaldiart[.]com/wp-includes/Requests/connection[.]php  
hxxp://castaldiart[.]com/wp-includes/Requests/Transport/connection[.]php  
hxxp://elevate[.]ae/wp-includes/IXR/connection[.]php  
hxxp://elevate[.]ae/wp-includes/customize/connection[.]php  
hxxp://koldpressjuice[.]com/wp-includes/IXR/connection[.]php  
hxxp://koldpressjuice[.]com/wp-includes/SimplePie/XML/connection[.]php  
hxxp://satwa[.]ae/wp-includes/images/connection[.]php  
hxxp://satwa[.]ae/wp-includes/rest-api/connection[.]php  
hxxp://soccertotsuae[.]com/wp-includes/Requests/Cookie/connection[.]php  
hxxp://soccertotsuae[.]com/wp-includes/Requests/Exception/connection[.]php  
hxxp://souqwalls[.]com/wp-includes/random\_compat/connection[.]php  
hxxp://souqwalls[.]com/wp-includes/theme-compat/connection[.]php  
hxxp://vintage[.]ae/wp-includes/random\_compat/connection[.]php  
hxxp://vintage[.]ae/wp-includes/pomo/connection[.]php  
hxxp://yogakidsuae[.]com/wp-includes/SimplePie/connection[.]php  
hxxp://yogakidsuae[.]com/wp-includes/SimplePie/XML/connection[.]php  
hxxp://binham[.]com/oxygen/connection[.]php  
hxxp://binham[.]com/artesia/connection[.]php  
hxxp://binhamgroup[.]com/Stopped/connection[.]php  
hxxp://binhamgroup[.]com/press/connection[.]php  
hxxp://mohamedbinham[.]com/wp-includes/connection[.]php  
hxxp://mohamedbinham[.]com/wp-includes/IXR/connection[.]php  
hxxp://thebedspace[.]com/wp-includes/Requests/connection[.]php  
hxxp://thebedspace[.]com/wp-includes/Requests/Response/connection[.]php  
hxxp://anythingispossible[.]world/wp-includes/IXR/connection[.]php  
hxxp://anythingispossible[.]world/wp-includes/Text/connection[.]php  
hxxp://ctteknik[.]com[.]tr/wp-content/themes/one-page/connection[.]php  
hxxp://ctteknik[.]com[.]tr/wp-includes/connection[.]php  
hxxp://acililan[.]net/libs/connection[.]php  
hxxp://stmgage[.]com/system/engine/connection[.]php  
hxxp://stmgage[.]com/system/config/connection[.]php  
hxxp://papyonplus[.]tv/css/connection[.]php  
hxxp://lavastandirustasi[.]com/includes/connection[.]php  
hxxp://www[.]cigercihamza[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://www[.]cigercihamza[.]com/wp-includes/connection[.]php  
hxxps://www[.]3bulut[.]net/wp-content/themes/arkahost/connection[.]php  
hxxps://www[.]3bulut[.]net/hizmetler/lang/connection[.]php

hxxp://gocekdaloshotel[.]com/sayfalar/connection[.]php  
hxxp://emrahucar[.]com[.]tr/wp-content/themes/rokophoto-lite/connection[.]php  
hxxp://emrahucar[.]com[.]tr/wp-includes/connection[.]php  
hxxp://www[.]fircasizaracyikama[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://www[.]fircasizaracyikama[.]com/wp-includes/connection[.]php  
hxxps://www[.]filthymindsco[.]com/wp-content/themes/twentyfifteen/inc/connection[.]php  
hxxps://www[.]filthymindsco[.]com/wp-includes/connection[.]php  
hxxp://kedidirkedi[.]com/wp-includes/connection[.]php  
hxxp://www[.]salonalara[.]com/wp-content/themes/twentyfifteen/inc/connection[.]php  
hxxp://www[.]salonalara[.]com/wp-includes/connection[.]php  
hxxp://www[.]ogreniver[.]com/wp-includes/connection[.]php  
hxxp://turhantarim[.]com/lang/connection[.]php  
hxxp://turhantarim[.]com/ik/inc/connection[.]php  
hxxp://www[.]mersinyedirenk[.]org/wp-content/themes/oxygen/connection[.]php  
hxxp://gayrimenkulvera[.]com/wp-content/themes/one-page/connection[.]php  
hxxp://gayrimenkulvera[.]com/wp-includes/connection[.]php  
hxxp://electrotoolbox[.]com/wp-content/themes/rowe/connection[.]php  
hxxp://www[.]cesikacatisistemleri[.]com/wp-content/themes/safirkurumsal/connection[.]php  
hxxp://www[.]cesikacatisistemleri[.]com/wp-includes/connection[.]php  
hxxp://almirayapim[.]com/wp-includes/connection[.]php  
hxxp://www[.]strancamagic[.]com/en/wp-includes/connection[.]php  
hxxp://raptiye[.]co/wp-includes/connection[.]php  
hxxp://safakhsap[.]com/fonksiyonlar/connection[.]php  
hxxp://safakhsap[.]com/resimler/semboller/connection[.]php  
hxxp://bursadanilan[.]com/iyzipay/samples/connection[.]php  
hxxp://www[.]cavgun[.]com/wp-includes/connection[.]php  
hxxp://ilanevim[.]com/kvitrin/connection[.]php  
hxxp://yelpazeinsaat[.]com[.]tr/plugins/finder/content/connection[.]php  
hxxp://kirkagac[.]bel[.]tr/sayfalar/connection[.]php  
hxxp://kirkagac[.]bel[.]tr/assets/fonts/connection[.]php  
hxxp://paybaskulu[.]com/fht/connection[.]php  
hxxp://www[.]ozsezerler[.]com/\_inc/connection[.]php  
hxxp://www[.]ozsezerler[.]com/en/connection[.]php  
hxxp://www[.]yapiborsasi[.]com/libs/connection[.]php  
hxxp://www[.]yapiborsasi[.]com/kvitrin/connection[.]php  
hxxps://boyaci-ustasi[.]com/wp-includes/connection[.]php  
hxxps://boyaci-ustasi[.]com/wp-content/themes/misty-lake/connection[.]php  
hxxp://www[.]altingunes[.]com/wp-includes/customize/connection[.]php  
hxxp://tamamsin[.]com/libs/connection[.]php  
hxxp://atlasins[.]com[.]tr/wp-includes/connection[.]php  
hxxp://atlasins[.]com[.]tr/wp-includes/connection[.]php  
hxxp://ilkerreklamcilik[.]com/Joomla\_site/includes/connection[.]php  
hxxp://luleburgazzob[.]org[.]tr/panel/plugins/ckeditor/plugins/link/dialogs/connection[.]php  
hxxp://burakgozutok[.]com/wp-content/themes/twentyfourteen/connection[.]php

hxxp://burakgozutok[.]com/wp-includes/connection[.]php  
hxxp://ekayapi[.]org/inc/connection[.]php  
hxxp://ekayapi[.]org/upload/connection[.]php  
hxxp://gdijital[.]com/libraries/connection[.]php  
hxxp://rumelipeyzaj[.]com/panel/connection[.]php  
hxxp://www[.]alpenfitil[.]com/wp-includes/connection[.]php  
hxxp://www[.]alpenfitil[.]com/wp-includes/connection[.]php  
hxxp://kindervilla[.]at/team/connection[.]php  
hxxp://www[.]ranzamodellerim[.]com/wp-content/plugins/contact-form-7/connection[.]php  
hxxp://www[.]metoikos-trade[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://tecnocoffee[.]com[.]tr/wp-content/themes/enlighten/connection[.]php  
hxxp://tecnocoffee[.]com[.]tr/wp-includes/connection[.]php  
hxxps://www[.]bedavasat[.]com/export/connection[.]php  
hxxps://www[.]bedavasat[.]com/iyzipay/src/lyzipay/connection[.]php  
hxxps://www[.]bedavasat[.]com/filesserver/connection[.]php  
hxxp://ustaariyorum[.]com[.]tr/wp-content/themes/wpfirma/connection[.]php  
hxxp://ustaariyorum[.]com[.]tr/wp-includes/connection[.]php  
hxxp://escapefromsofa[.]com/theme/efs/connection[.]php  
hxxp://escapefromsofa[.]com/ajax/connection[.]php  
hxxp://ozmetalpen[.]com/wp-includes/connection[.]php  
hxxp://nevzatsolmazinsaat[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://nevzatsolmazinsaat[.]com/wp-includes/connection[.]php  
hxxp://standartdogalgaz[.]com/wp-includes/connection[.]php  
hxxp://starttr[.]com/system/library/connection[.]php  
hxxp://www[.]karavansyahat[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://reklambasvurusu[.]com/sistem/connection[.]php  
hxxp://reklambasvurusu[.]com!/ercer2001/sistem/connection[.]php  
hxxp://www[.]emlakbizden[.]com/libs/connection[.]php  
hxxp://rentacarline[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://www[.]pergolatentefiyatlar[.]com/wp-includes/connection[.]php  
hxxp://www[.]oroazteca[.]net/wp-includes/connection[.]php  
hxxp://markizorganizasyon[.]com/wp-includes/connection[.]php  
hxxp://markizorganizasyon[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://akin[.]me/wp-includes/connection[.]php  
hxxp://akin[.]me/wp-content/themes/founder/connection[.]php  
hxxp://www[.]bogazturu[.]net/includes/connection[.]php  
hxxp://onurlergayrimenkul[.]com/application/language/english/connection[.]php  
hxxp://www[.]a-zgrup[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://www[.]a-zgrup[.]com/wp-includes/connection[.]php  
hxxp://matmazel-gelinlik[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://www[.]gokkubbe[.]biz/wp-includes/connection[.]php  
hxxp://eraslan[.]com[.]tr/en/about/connection[.]php  
hxxp://eraslan[.]com[.]tr/en/history/assets/nokta/css/connection[.]php  
hxxp://www[.]hibedanis[.]com/en/\_ajax/connection[.]php

hxxp://www[.]hibedanis[.]com/en/\_inc/connection[.]php  
hxxp://yildizgokart[.]com/wp-content/plugins/contact-form-7/includes/connection[.]php  
hxxp://cinarli[.]com/catering/img/connection[.]php  
hxxp://cinarli[.]com/restaurant/captcha/connection[.]php  
hxxp://alyanslife[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://alyanslife[.]com/wp-includes/connection[.]php  
hxxp://www[.]hibedanis[.]com/admin/connection[.]php  
hxxp://www[.]hibedanis[.]com/en/\_inc/connection[.]php  
hxxp://yildizgokart[.]com/wp-content/languages/plugins/connection[.]php  
hxxp://acililan[.]net/libs/connection[.]php  
hxxp://stmgage[.]com/system/engine/connection[.]php  
hxxp://novusglobal[.]us/templates/zoner/connection[.]php  
hxxp://1111crm[.]com/3Party/ckeditor/plugins/bidi/lang/connection[.]php  
hxxp://1111crm[.]com/ESKI/loginbox/system/connection[.]php  
hxxp://rehberhds[.]com/wp-includes/connection[.]php  
hxxp://ngvisco[.]com/wp-includes/connection[.]php  
hxxp://ngvisco[.]com/wp-content/themes/betheme/connection[.]php  
hxxp://kursunkalemhoca[.]com/wp-content/themes/twentyseventeen/connection[.]php  
hxxps://www[.]asortie[.]com/blog/wp-content/themes/colormag/connection[.]php  
hxxps://www[.]asortie[.]com/blog/wp-includes/connection[.]php  
hxxps://bayanhobisi[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxps://bayanhobisi[.]com/wp-includes/connection[.]php  
hxxp://3eyonetim[.]com/wp-includes/connection[.]php  
hxxp://3eyonetim[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://derinbutikotel[.]com/templates/bee3/language/en-GB/connection[.]php  
hxxp://minitalya[.]com/wp-content/languages/plugins/connection[.]php  
hxxp://www[.]armateknolojimerkezi[.]com/wp-includes/pomo/connection[.]php  
hxxp://www[.]armateknolojimerkezi[.]com/wp-content/languages/plugins/connection[.]php  
hxxp://www[.]eogren[.]me/wp-includes/widgets/connection[.]php  
hxxp://www[.]eogren[.]me/wp-content/languages/plugins/connection[.]php  
hxxp://www[.]inalhukukburosu[.]com/wp-includes/widgets/connection[.]php  
hxxp://www[.]inalhukukburosu[.]com/wp-content/languages/plugins/connection[.]php  
hxxp://www[.]osmaniyesevgi[.]com[.]tr/wp-includes/pomo/connection[.]php  
hxxp://www[.]osmaniyesevgi[.]com[.]tr/wp-content/languages/plugins/connection[.]php  
hxxp://ercekagit[.]com/wp-includes/widgets/connection[.]php  
hxxp://ercekagit[.]com/wp-content/languages/plugins/connection[.]php  
hxxp://lubesoltr[.]com/images/connection[.]php  
hxxp://watergreen[.]com[.]tr/pages/inc/connection[.]php  
hxxp://watergreen[.]com[.]tr/lib/ckeditor/plugins/a11yhelp/dialogs/connection[.]php  
hxxp://tamirdeyiz[.]com/plugins/extension/joomla/connection[.]php  
hxxp://tamirdeyiz[.]com/language/tr-TR/connection[.]php  
hxxp://www[.]finansalkredi[.]com/wp-includes/widgets/connection[.]php  
hxxp://www[.]finansalkredi[.]com/wp-content/languages/plugins/connection[.]php

hxxps://dogruwebtasarim[.]com/ortak/editable/bootstrap3/1[.]5[.]1/bootstrap3-  
editable/css/connection[.]php  
hxxps://dogruwebtasarim[.]com/ortak/seourl/1[.]7[.]1/connection[.]php  
hxxp://er-emmakine[.]com[.]tr/admin/include/connection[.]php  
hxxp://er-emmakine[.]com[.]tr/admin/chat/documentation/css/connection[.]php  
hxxp://turanlarcitsistemleri[.]com/wp-includes/pomo/connection[.]php  
hxxp://turanlarcitsistemleri[.]com/wp-content/languages/plugins/connection[.]php  
hxxp://www[.]uzaktanogrenin[.]com/phpmailer/connection[.]php  
hxxp://www[.]uzaktanogrenin[.]com/css/presets/connection[.]php  
hxxp://e-learning[.]secilenlernetwork[.]com/phpmailer/connection[.]php  
hxxp://e-learning[.]secilenlernetwork[.]com/yonetim/ckeditor/plugins/about/dialogs/connection[.]php  
hxxp://luleburgazvinc[.]com/mail/connection[.]php  
hxxp://luleburgazvinc[.]com/panel/plugins/ckeditor/connection[.]php  
hxxp://www[.]karamesetarim[.]com/wp-includes/widgets/connection[.]php  
hxxp://www[.]karamesetarim[.]com/wp-content/languages/plugins/connection[.]php  
hxxp://teknodizayn[.]net/domain/js/connection[.]php  
hxxp://teknodizayn[.]net/baglan/facebook/src/connection[.]php  
hxxp://www[.]hankimya[.]com/wp-includes/pomo/connection[.]php  
hxxp://www[.]hankimya[.]com/wp-content/languages/plugins/connection[.]php  
hxxp://hasatvet[.]com[.]tr/ekatalog/lib/connection[.]php  
hxxp://hasatvet[.]com[.]tr/insantr/language/connection[.]php  
hxxp://emelcekici[.]com/engine/connection[.]php  
hxxp://emelcekici[.]com/engine/ajax/connection[.]php  
hxxp://tamer[.]info/dle/engine/ajax/connection[.]php  
hxxp://tamer[.]info/dle/engine/connection[.]php  
hxxp://seyekanakliyat[.]com/cgi-bin/connection[.]php  
hxxp://www[.]sendogansevda[.]com/wp-includes/widgets/connection[.]php  
hxxp://www[.]sendogansevda[.]com/wp-content/languages/plugins/connection[.]php  
hxxp://viranlar[.]com/func/connection[.]php  
hxxp://viranlar[.]com/fancybox/connection[.]php  
hxxp://mimart1984[.]com/panel/plugins/chartjs/connection[.]php  
hxxp://mimart1984[.]com/panel/dist/css/skins/connection[.]php  
hxxp://nurbahcemakinalari[.]com/epiksel/epiksel\_admin\_shortcuts/css/connection[.]php  
hxxp://nurbahcemakinalari[.]com/override/export/admin/controller/common/connection[.]php  
hxxp://safacaliskan[.]com/wp-includes/widgets/connection[.]php  
hxxp://safacaliskan[.]com/wp-content/languages/plugins/connection[.]php  
hxxps://www[.]eimza[.]gen[.]tr/images/yedek/connection[.]php  
hxxps://www[.]eimza[.]gen[.]tr/class/mail/connection[.]php  
hxxp://organigiz[.]org/wp-includes/widgets/connection[.]php  
hxxp://organigiz[.]org/wp-content/languages/plugins/connection[.]php  
hxxp://www[.]tekirdagbulten[.]com/wp-includes/widgets/connection[.]php  
hxxp://www[.]tekirdagbulten[.]com/wp-content/languages/plugins/connection[.]php  
hxxp://arkadasariyoruz[.]com/reklamlar/connection[.]php  
hxxp://arkadasariyoruz[.]com/mudur/connection[.]php

hxxp://mywishlistapp[.]com/sanal/fonts/codropsicons/connection[.]php  
hxxp://mywishlistapp[.]com/kaynak/dist/stylesheets/connection[.]php  
hxxp://tafitur[.]com/muhasebe/plugins/chart/connection[.]php  
hxxp://tafitur[.]com/muhasebe/plugins/advanced-datatable/css/connection[.]php  
hxxp://www[.]ddcreklam[.]com/wp-content/languages/plugins/connection[.]php  
hxxp://www[.]ddcreklam[.]com/wp-includes/widgets/connection[.]php  
hxxp://gulucuk[.]com[.]tr/panel/assess/images/connection[.]php  
hxxp://gulucuk[.]com[.]tr/rs-plugin/assets/connection[.]php  
hxxp://fatihguvenmotor[.]com/wp-includes/widgets/connection[.]php  
hxxp://fatihguvenmotor[.]com/wp-content/languages/plugins/connection[.]php  
hxxp://banaherseylazim[.]com/catalog/view/javascript/jquery/connection[.]php  
hxxp://banaherseylazim[.]com/system/config/connection[.]php  
hxxp://nikahsepetim[.]com/catalog/view/javascript/jquery/connection[.]php  
hxxp://nikahsepetim[.]com/blog/wp-includes/widgets/connection[.]php  
hxxp://www[.]ozankaratas[.]com/wp-includes/widgets/connection[.]php  
hxxp://www[.]ozankaratas[.]com/wp-content/languages/plugins/connection[.]php  
hxxp://salonaltinmakas[.]com/cgi-bin/connection[.]php  
hxxp://salonaltinmakas[.]com/assets/js/connection[.]php  
hxxp://buldurgrup[.]com/plugins/captcha/recaptcha/connection[.]php  
hxxp://buldurgrup[.]com/libraries/cms/application/connection[.]php  
hxxp://gebekulubu[.]com/fonts/alice/connection[.]php  
hxxp://gebekulubu[.]com/core/cpstyles/vBulletin\_5\_Default/connection[.]php  
hxxp://isikpolyester[.]com/css/custom-theme/images/connection[.]php  
hxxp://isikpolyester[.]com/graphics/iletisim/connection[.]php  
hxxp://bayramturgutnakliyat[.]com[.]tr/components/com\_ajax/connection[.]php  
hxxp://bayramturgutnakliyat[.]com[.]tr/libraries/cms/component/router/rules/connection[.]php  
hxxp://perdemis[.]com/panel/ckeditor/\_samples/adobear/connection[.]php  
hxxp://perdemis[.]com/panel/ckeditor/plugins/forms/dialogs/connection[.]php  
hxxp://ersagurunlerisatis[.]com/cgi-bin/connection[.]php  
hxxp://ersagurunlerisatis[.]com/style/bakim/tools/socicon/font/connection[.]php  
hxxp://naturagro[.]com[.]tr/calisma/assets/css/connection[.]php  
hxxp://naturagro[.]com[.]tr/calisma/modules/images/prettyPhoto/dark\_rounded/connection[.]php  
hxxps://www[.]owletmedikal[.]com/manager/js/advanced-datatable/css/connection[.]php  
hxxps://www[.]owletmedikal[.]com/manager/php-  
activerecord/examples/orders/models/connection[.]php  
hxxps://yemekler[.]com[.]tr/wp-includes/Requests/Exception/hxxp/connection[.]php  
hxxps://yemekler[.]com[.]tr/wp-content/languages/plugins/connection[.]php  
hxxps://pentilon[.]com/wp-includes/widgets/connection[.]php  
hxxps://pentilon[.]com/wp-content/languages/plugins/connection[.]php  
hxxps://bestpa[.]com[.]tr/catalog/view/theme/default/stylesheet/connection[.]php  
hxxps://bestpa[.]com[.]tr/catalog/view/theme/default/stylesheet/connection[.]php  
hxxp://eylulprefabrik[.]com/images/connection[.]php  
hxxp://eylulprefabrik[.]com/cgi-bin/connection[.]php  
hxxp://kralicemmasaj[.]com/layouts/libraries/cms/html/bootstrap/connection[.]php

hxxp://www[.]nilgunakkok[.]com/wp-includes/widgets/connection[.]php  
hxxp://www[.]orgutigisimodelleri[.]com/wp-includes/pomo/connection[.]php  
hxxp://anadolutente[.]com[.]tr/js/connection[.]php  
hxxp://anadolutente[.]com[.]tr/fonts/connection[.]php  
hxxp://entpsoft[.]com/cgi-bin/connection[.]php  
hxxp://entpsoft[.]com/LISP-SURELERI/connection[.]php  
hxxp://besiktasgorselsanatlari[.]com/loginbox/app/connection[.]php  
hxxp://besiktasgorselsanatlari[.]com/loginbox/3party/ckeditor/plugins/a11yhelp/dialogs/connection[.]php  
hxxp://ilkadim[.]k12[.]tr/media/contacts/connection[.]php  
hxxp://senollarturizm[.]com[.]tr/vendor/scripts/jquery/connection[.]php  
hxxp://arabaemlak[.]com/magaza/cgi-bin/connection[.]php  
hxxp://www[.]ankarahaliyikamafirmalari[.]web[.]tr/wp-includes/widgets/connection[.]php  
hxxp://www[.]ankarahaliyikamafirmalari[.]web[.]tr/wp-includes/js/jquery/ui/connection[.]php  
hxxp://en[.]nordiksimit[.]org/wp-includes/widgets/connection[.]php  
hxxp://en[.]nordiksimit[.]org/wp-includes/js/jquery/ui/connection[.]php  
hxxp://dyosanayiboyalari[.]com/cgi-bin/connection[.]php  
hxxp://www[.]ufukdesign[.]com/wp-includes/js/jquery/ui/connection[.]php  
hxxp://mehmetak[.]in/cgi-bin/connection[.]php  
hxxp://teknobi[.]net/include/payu/CLASSES/connection[.]php  
hxxp://www[.]ilanbas[.]com/panel/js/connection[.]php  
hxxp://ilanbas[.]com//js/bxslider/images/connection[.]php  
hxxp://gunluoglumobilya[.]com/system/config/connection[.]php  
hxxp://gunluoglumobilya[.]com/catalog/view/javascript/jquery/ui/connection[.]php  
hxxp://www[.]oyun16[.]com/libs/plugins/connection[.]php  
hxxp://www[.]oyun16[.]com/den/css/connection[.]php  
hxxp://papyonplus[.]tv/dummy/connection[.]php  
hxxp://papyonplus[.]tv/css/connection[.]php  
hxxp://lavastandirustasi[.]com/includes/connection[.]php  
hxxp://lavastandirustasi[.]com/cli/connection[.]php  
hxxp://www[.]cigercihamza[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://www[.]cigercihamza[.]com/wp-includes/connection[.]php  
hxxps://www[.]3bulut[.]net/wp-content/themes/arkahost/connection[.]php  
hxxps://www[.]3bulut[.]net/hizmetler/lang/connection[.]php  
hxxp://akinbilgisayarumraniye[.]com/inc/connection[.]php  
hxxp://akinbilgisayarumraniye[.]com/sistem/elfinder/connectors/php/connection[.]php  
hxxp://gocekdaloshotel[.]com/dil/connection[.]php  
hxxp://gocekdaloshotel[.]com/sayfalar/connection[.]php  
hxxp://emrahucar[.]com[.]tr/wp-content/themes/rokophoto-lite/connection[.]php  
hxxp://emrahucar[.]com[.]tr/wp-includes/connection[.]php  
hxxp://www[.]fircasizaracyikama[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://www[.]fircasizaracyikama[.]com/wp-includes/connection[.]php  
hxxps://www[.]filthymindsco[.]com/wp-content/themes/twentyfifteen/inc/connection[.]php  
hxxps://www[.]filthymindsco[.]com/wp-includes/connection[.]php  
hxxp://www[.]bulutuzer[.]com/wp-content/themes/twentyfifteen/connection[.]php



hxxp://www[.]bulutuzer[.]com/wp-includes/connection[.]php  
hxxp://mavioksidan[.]net/admin/view/javascript/openbay/css/connection[.]php  
hxxp://mavioksidan[.]net/catalog/model/affiliate/connection[.]php  
hxxp://halilbalyapi[.]com/includes/connection[.]php  
hxxp://halilbalyapi[.]com/language/en-GB/connection[.]php  
hxxp://kedidirkedi[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://kedidirkedi[.]com/wp-includes/connection[.]php  
hxxp://www[.]salonalara[.]com/wp-content/themes/twentyfifteen/inc/connection[.]php  
hxxp://www[.]salonalara[.]com/wp-includes/connection[.]php  
hxxp://dsmartbursa[.]net/\_frame/connection[.]php  
hxxp://dsmartbursa[.]net/\_iserv/form2mail/connection[.]php  
hxxp://www[.]ogreniver[.]com/wp-content/themes/metro-creativex/connection[.]php  
hxxp://www[.]ogreniver[.]com/wp-includes/connection[.]php  
hxxp://mangalaburada[.]com/wp-content/themes/idoneita/connection[.]php  
hxxp://mangalaburada[.]com/wp-includes/connection[.]php  
hxxp://www[.]ozeliletisim[.]com[.]tr/wp-includes/connection[.]php  
hxxp://www[.]pastacikadin[.]com/wp-content/themes/bulan/connection[.]php  
hxxp://www[.]pastacikadin[.]com/wp-includes/connection[.]php  
hxxp://turhantarim[.]com/lang/connection[.]php  
hxxp://turhantarim[.]com/ik/inc/connection[.]php  
hxxp://www[.]mersinyedirenk[.]org/wp-content/themes/oxygen/connection[.]php  
hxxp://www[.]mersinyedirenk[.]org/wp-includes/connection[.]php  
hxxp://gayrimenkulvera[.]com/wp-content/themes/one-page/connection[.]php  
hxxp://gayrimenkulvera[.]com/wp-includes/connection[.]php  
hxxp://projemsoft[.]com/includes/twitter/connection[.]php  
hxxp://projemsoft[.]com/js/connection[.]php  
hxxp://electrotoolbox[.]com/wp-content/themes/rowe/connection[.]php  
hxxp://electrotoolbox[.]com/wp-includes/connection[.]php  
hxxp://www[.]cesikacatisistemleri[.]com/wp-content/themes/safirkurumsal/connection[.]php  
hxxp://www[.]cesikacatisistemleri[.]com/wp-includes/connection[.]php  
hxxp://almirayapim[.]com/wp-content/themes/minamaze/connection[.]php  
hxxp://almirayapim[.]com/wp-includes/connection[.]php  
hxxp://www[.]strancamagic[.]com/en/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://www[.]strancamagic[.]com/en/wp-includes/connection[.]php  
hxxp://www[.]marufymm[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://www[.]marufymm[.]com/wp-includes/connection[.]php  
hxxp://ayyildizmimari[.]com/ders/inc/connection[.]php  
hxxp://ayyildizmimari[.]com/bakim/connection[.]php  
hxxp://raptiye[.]co/wp-content/themes/illyd/connection[.]php  
hxxp://raptiye[.]co/wp-includes/connection[.]php  
hxxp://safakhsap[.]com/fonksiyonlar/connection[.]php  
hxxp://safakhsap[.]com/resimler/semboller/connection[.]php  
hxxp://bursadanilan[.]com/eski/libs/connection[.]php  
hxxp://bursadanilan[.]com/iyzipay/samples/connection[.]php

hxxp://www[.]cavgun[.]com/wp-content/themes/tema/connection[.]php  
hxxp://www[.]cavgun[.]com/wp-includes/connection[.]php  
hxxp://www[.]ilanevim[.]com/mobil/connection[.]php  
hxxp://ilanevim[.]com/kvitrin/connection[.]php  
hxxp://yelpazeinsaat[.]com[.]tr/plugins/finder/content/connection[.]php  
hxxp://yelpazeinsaat[.]com[.]tr/yeni/plugins/finder/content/connection[.]php  
hxxp://safasengezer[.]com[.]tr/wp-includes/connection[.]php  
hxxp://kirkagac[.]bel[.]tr/sayfalar/connection[.]php  
hxxp://kirkagac[.]bel[.]tr/assets/fonts/connection[.]php  
hxxp://7likurbanbaskulu[.]com/hassas/connection[.]php  
hxxp://7likurbanbaskulu[.]com/tartim/connection[.]php  
hxxp://paybaskulu[.]com/tartim/connection[.]php  
hxxp://paybaskulu[.]com/fht/connection[.]php  
hxxp://kurbanhissebaskulu[.]net/barkodlular/connection[.]php  
hxxp://kurbanhissebaskulu[.]net/tartim/connection[.]php  
hxxp://www[.]ozsezerler[.]com/\_inc/connection[.]php  
hxxp://www[.]ozsezerler[.]com/en/connection[.]php  
hxxp://www[.]yapiborsasi[.]com/libs/connection[.]php  
hxxp://www[.]yapiborsasi[.]com/kvitrin/connection[.]php  
hxxps://boyaci-ustasi[.]com/wp-includes/connection[.]php  
hxxps://boyaci-ustasi[.]com/wp-content/themes/misty-lake/connection[.]php  
hxxp://www[.]altingunes[.]com/wp-includes/connection[.]php  
hxxp://www[.]altingunes[.]com/wp-includes/customize/connection[.]php  
hxxp://www[.]tamamsin[.]com/panel/connection[.]php  
hxxp://tamamsin[.]com/libs/connection[.]php  
hxxp://tamamsin[.]com/dil/connection[.]php  
hxxp://atlasins[.]com[.]tr/wp-includes/connection[.]php  
hxxp://atlasins[.]com[.]tr/wp-includes/connection[.]php  
hxxp://ilkerreklamcilik[.]com/Joomla\_site/cli/connection[.]php  
hxxp://ilkerreklamcilik[.]com/Joomla\_site/includes/connection[.]php  
hxxp://viparkcenter[.]com/wp-includes/connection[.]php  
hxxp://viparkcenter[.]com/wp-content/themes/twentyseventeen/connection[.]php  
hxxp://www[.]klavyebende[.]com/wp-content/themes/spasalon/connection[.]php  
hxxp://www[.]klavyebende[.]com/wp-includes/connection[.]php  
hxxp://luleburgazzob[.]org[.]tr/panel/plugins/ckeditor/plugins/about/dialogs/hidpi/connection[.]php  
hxxp://luleburgazzob[.]org[.]tr/panel/plugins/ckeditor/plugins/link/dialogs/connection[.]php  
hxxp://burakgozutok[.]com/wp-content/themes/twentyfourteen/connection[.]php  
hxxp://burakgozutok[.]com/wp-includes/connection[.]php  
hxxp://gebzehalandirmatr[.]com/admin/connection[.]php  
hxxp://gebzehalandirmatr[.]com/yedek/captcha/connection[.]php  
hxxp://deltasolar[.]com[.]tr/admin/connection[.]php  
hxxp://deltasolar[.]com[.]tr/catalog/controller/api/connection[.]php  
hxxp://ekayapi[.]org/inc/connection[.]php  
hxxp://ekayapi[.]org/upload/connection[.]php

hxxp://www[.]otocekicidenizli[.]com/wp-admin/connection[.]php  
hxxp://www[.]otocekicidenizli[.]com/wp-content/themes/twentyfourteen/connection[.]php  
hxxp://cevahirkardesler[.]com[.]tr/gazete/pages/connection[.]php  
hxxp://cevahirkardesler[.]com[.]tr/themes/1/connection[.]php  
hxxp://gdijital[.]com/administrator/connection[.]php  
hxxp://gdijital[.]com/libraries/connection[.]php  
hxxp://rumelipeyzaj[.]com/panel/connection[.]php  
hxxp://rumelipeyzaj[.]com/sayfalar/connection[.]php  
hxxp://www[.]alpenfital[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://www[.]alpenfital[.]com/wp-includes/connection[.]php  
hxxp://www[.]alpenfital[.]com/wp-includes/connection[.]php  
hxxp://kindervilla[.]at/team/admin/connection[.]php  
hxxp://mslvinc[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://kindervilla[.]at/team/connection[.]php  
hxxp://mslvinc[.]com/wp-includes/connection[.]php  
hxxp://www[.]ranzamodellerim[.]com/wp-content/plugins/contact-form-7/connection[.]php  
hxxp://www[.]ranzamodellerim[.]com/wp-includes/connection[.]php  
hxxp://www[.]metoikos-trade[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://www[.]metoikos-trade[.]com/wp-includes/connection[.]php  
hxxp://tecnocoffee[.]com[.]tr/wp-content/themes/enlighten/connection[.]php  
hxxp://tecnocoffee[.]com[.]tr/wp-includes/connection[.]php  
hxxps://www[.]bedavasat[.]com/export/connection[.]php  
hxxps://www[.]bedavasat[.]com/iyzipay/src/lyzipay/connection[.]php  
hxxps://www[.]bedavasat[.]com/fileservers/connection[.]php  
hxxp://ustaariyorum[.]com[.]tr/wp-content/themes/wpfirma/connection[.]php  
hxxp://ustaariyorum[.]com[.]tr/wp-includes/connection[.]php  
hxxp://escapefromsofa[.]com/theme/efs/connection[.]php  
hxxp://escapefromsofa[.]com/ajax/connection[.]php  
hxxp://www[.]ozturkormancilik[.]com[.]tr/wp-content/themes/twentyfourteen/connection[.]php  
hxxp://www[.]ozturkormancilik[.]com[.]tr/wp-includes/connection[.]php  
hxxp://trakyacepteknik[.]com/tema/telefon/vendor/assets/connection[.]php  
hxxp://trakyacepteknik[.]com/tema/telefon/fonts/font-awesome/css/connection[.]php  
hxxp://asortiemobilya[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://asortiemobilya[.]com/wp-includes/Text/connection[.]php  
hxxp://ozmetalpen[.]com/wp-content/themes/twentyfourteen/connection[.]php  
hxxp://ozmetalpen[.]com/wp-includes/connection[.]php  
hxxp://nevzatsolmazinsaat[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://nevzatsolmazinsaat[.]com/wp-includes/connection[.]php  
hxxp://standartdogalgaz[.]com/wp-content/themes/themo/connection[.]php  
hxxp://standartdogalgaz[.]com/wp-includes/connection[.]php  
hxxp://startr[.]com/admin/connection[.]php  
hxxp://startr[.]com/system/library/connection[.]php  
hxxp://birtavsiyemvar[.]com/assets/css/connection[.]php  
hxxp://birtavsiyemvar[.]com/assets/js/connection[.]php

hxxp://www[.]karavanseyahat[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://www[.]karavanseyahat[.]com/wp-includes/connection[.]php  
hxxp://reklambasvurusu[.]com/sistem/connection[.]php  
hxxp://reklambasvurusu[.]com/!ercer2001/sistem/connection[.]php  
hxxp://www[.]ckumas[.]com/wp-admin/connection[.]php  
hxxp://www[.]ckumas[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://www[.]ckumas[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://www[.]jilksahibinden[.]com/kvitrin/connection[.]php  
hxxp://www[.]jilksahibinden[.]com/mobil/connection[.]php  
hxxp://www[.]emlakbizden[.]com/libs/connection[.]php  
hxxp://www[.]emlakbizden[.]com/templates/yedekparca/images/connection[.]php  
hxxp://enerjiport[.]org/wp-includes/connection[.]php  
hxxp://enerjiport[.]org/wp-content/themes/twentyseventeen/connection[.]php  
hxxp://rentacarline[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://rentacarline[.]com/wp-includes/connection[.]php  
hxxp://www[.]akillipati[.]com/wp-content/themes/colormag/connection[.]php  
hxxp://www[.]akillipati[.]com/wp-includes/connection[.]php  
hxxp://www[.]pergolatentefiyatlari[.]com/wp-content/themes/twentyseventeen/connection[.]php  
hxxp://www[.]pergolatentefiyatlari[.]com/wp-includes/connection[.]php  
hxxp://www[.]oroazteca[.]net/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://www[.]oroazteca[.]net/wp-includes/connection[.]php  
hxxp://markizorganizasyon[.]com/wp-includes/connection[.]php  
hxxp://markizorganizasyon[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://akin[.]me/wp-includes/connection[.]php  
hxxp://akin[.]me/wp-content/themes/founder/connection[.]php  
hxxp://www[.]bogazturu[.]net/includes/connection[.]php  
hxxp://www[.]bogazturu[.]net/plugins/content/finder/connection[.]php  
hxxp://onurlergayrimenkul[.]com/application/language/english/connection[.]php  
hxxp://onurlergayrimenkul[.]com/themes/3d-blue-portal/library/connection[.]php  
hxxp://stsiletisim[.]com/admin/connection[.]php  
hxxp://stsiletisim[.]com/sistem/connection[.]php  
hxxp://www[.]a-zgrup[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://www[.]a-zgrup[.]com/wp-includes/connection[.]php  
hxxp://matmazel-gelinlik[.]com/wp-includes/connection[.]php  
hxxp://matmazel-gelinlik[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://www[.]gokkubbe[.]biz/wp-includes/connection[.]php  
hxxp://www[.]gokkubbe[.]biz/wp-content/themes/Extra/connection[.]php  
hxxp://eraslan[.]com[.]tr/en/about/connection[.]php  
hxxp://eraslan[.]com[.]tr/en/history/assets/nokta/css/connection[.]php  
hxxp://www[.]hibedanis[.]com/en/\_ajax/connection[.]php  
hxxp://www[.]hibedanis[.]com/en/\_inc/connection[.]php  
hxxp://yildizgokart[.]com/wp-content/plugins/contact-form-7/includes/connection[.]php  
hxxp://yildizgokart[.]com/wp-includes/connection[.]php  
hxxp://cinarli[.]com/catering/img/connection[.]php

hxxp://cinarli[.]com/restaurant/captcha/connection[.]php  
hxxp://sumder[.]org/wp-content/themes/sumder/connection[.]php  
hxxp://sumder[.]org/wp-includes/connection[.]php  
hxxp://alyanslife[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://alyanslife[.]com/wp-includes/connection[.]php  
hxxp://www[.]hibedanis[.]com/admin/connection[.]php  
hxxp://www[.]hibedanis[.]com/en/\_inc/connection[.]php  
hxxp://yildizgokart[.]com/wp-content/languages/plugins/connection[.]php  
hxxp://yildizgokart[.]com/wp-includes/connection[.]php  
hxxp://acililan[.]net/libs/connection[.]php  
hxxp://www[.]goldenplus[.]com[.]tr/\_inc/connection[.]php  
hxxp://qrme[.]site/wp-content/themes/twentyseventeen/connection[.]php  
hxxp://qrme[.]site/wp-includes/connection[.]php  
hxxp://stmgage[.]com/system/engine/connection[.]php  
hxxp://stmgage[.]com/system/config/connection[.]php  
hxxp://novusglobal[.]us/templates/zoner/connection[.]php  
hxxp://novusglobal[.]us/yonet/includes/connection[.]php  
hxxp://1111crm[.]com/3Party/ckeditor/plugins/bidi/lang/connection[.]php  
hxxp://1111crm[.]com/ESKI/loginbox/system/connection[.]php  
hxxp://rehberhds[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://rehberhds[.]com/wp-includes/connection[.]php  
hxxp://ctteknik[.]com[.]tr/wp-content/themes/one-page/connection[.]php  
hxxp://ctteknik[.]com[.]tr/wp-includes/connection[.]php  
hxxp://ngvisco[.]com/wp-includes/connection[.]php  
hxxp://ngvisco[.]com/wp-content/themes/betheme/connection[.]php  
hxxp://kursunkalemhoca[.]com/wp-content/themes/twentyseventeen/connection[.]php  
hxxp://kursunkalemhoca[.]com/wp-includes/connection[.]php  
hxxps://www[.]asortie[.]com/blog/wp-content/themes/colormag/connection[.]php  
hxxps://www[.]asortie[.]com/blog/wp-includes/connection[.]php  
hxxp://www[.]tulayalpayegitim[.]com/wp-content/themes/einsteiniumist/connection[.]php  
hxxp://www[.]tulayalpayegitim[.]com/wp-includes/customize/connection[.]php  
hxxps://bayanhobisi[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxps://bayanhobisi[.]com/wp-includes/connection[.]php  
hxxp://3eyonetim[.]com/wp-includes/connection[.]php  
hxxp://3eyonetim[.]com/wp-content/themes/twentyfifteen/connection[.]php  
hxxp://derinbutikotel[.]com/templates/bee3/language/en-GB/connection[.]php  
hxxp://derinbutikotel[.]com/includes/connection[.]php

## **Clearing the MuddyWater - Analysis of new MuddyWater Samples**

---

## **PRB-Backdoor - A Fully Loaded PowerShell Backdoor with Evil Intentions**

---