Muddying the Water: Targeted Attacks in the Middle East

By Tom Lancaster

Published: 2017-11-14 · Archived: 2026-04-05 14:44:07 UTC

Summary
This blog discusses targeted attacks against the Middle East taking place between February and October 2017 by a group Unit 42 is naming "MuddyWater". This blog links this recent activity with previous isolated public reporting on similar attacks we believe are related. We refer to these attacks as MuddyWater due to the confusion in attributing these attacks. Although the activity was previously linked by others to the FIN7 threat actor group, our research suggests the activity is in fact espionage related and unlikely to be FIN7 related.
The MuddyWater attacks are primarily against Middle Eastern nations. However, we have also observed attacks against surrounding nations and beyond, including targets in India and the USA. MuddyWater attacks are characterized by the use of a slowly evolving PowerShell-based first stage backdoor we call “POWERSTATS”. Despite broad scrutiny and reports on MuddyWater attacks, the activity continues with only incremental changes to the tools and techniques.

Introduction & Overview

The Palo Alto Networks Unit 42 research team recently came across a series of malicious files which were almost identical to those targeting the Saudi Arabian government previously discussed by MalwareBytes. Which in turn, closely resembles a previous article by Morphisec. These attacks have also been tracked by several other researchers on Twitter and elsewhere.
The activity has been consistent throughout 2017 and, based on our analysis, targets or is suspected to target, entities in the following countries:

- Saudi Arabia
- Iraq
- Israel
- United Arab Emirates
- Georgia
- India
- Pakistan
- Turkey
- USA

The malicious documents were adjusted according to the target regions, often using the logos of branches of local government, prompting the users to bypass security controls and enable macros. An overview of the technical changes seen in the past year is given in the graphic below, note that raw IOCs present in this graphic can be

found as text in the Appendix at the end of this article.

Nov

Delivery method
- Dropped directly from Macros

POWERSTATS C2 IP
- GET, 148.251.204.131:8060/?p=$customb64encodedstring

POWERSTATS proxy URLs
- Additional proxy URLs added **(see Appendix C)**

Other
- **Anti-Sandbox:** The malware delays execution for 1hr if no ".dat" file is present in "C:\Users\Public\Documents\"

Oct

Delivery method
- Dropped directly from macros

POWERSTATS C2 IP
- GET, 148.251.204.131:8060/?p=$customb64encodedstring

POWERSTATS proxy URLs
- Use of **new Proxy URLs** (see Appendix C)

Other
- **Code obfuscation** with open source tool Invoke-Obfuscation
- **Anti-Analysis** : checks running processes for known debugging and analysis tools – exits if found, example processes searched for include:
  - ollydbg, ProcessHacker, tcpview, procmon, procexp, idaq, wireshark, etc.

Late Sept to early Oct

Delivery method
- Downloaded from file sharing sites, such as **Pastebin** and **Filebin** via macro

POWERSTATS C2 IP
- GET, 144.76.109.88:80/al/?action=

POWERSTATS proxy URLs
- Use of known proxy URLs (previous reporting)

Sept

Delivery method
- **Downloaded via macro from GitHub profiles** (described later), hosted on GitHub as PS2EXE binaries and raw .ps1 files

POWERSTATS C2 IP
- Unidentified

POWERSTATS proxy URLs
- Use of known proxy URLs (previous reporting)

Delivery method

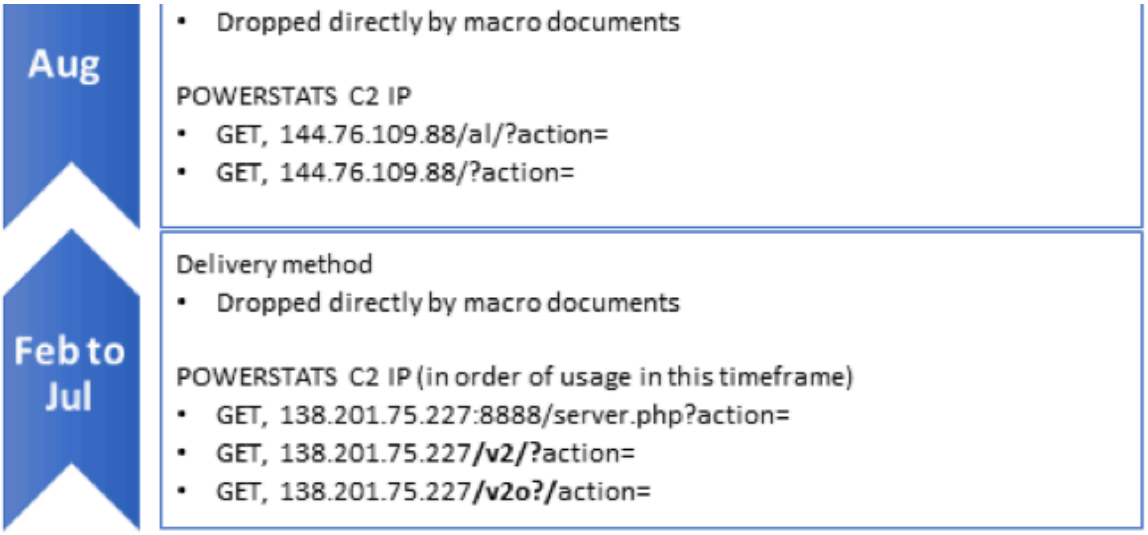

Figure 1. An overview of the delivery of POWERSTATS, C2 URLs used, and other changes in the malware

MuddyWater in the Middle East

The attackers behind MuddyWater have been active throughout 2017, with targets across the Middle East and surrounding areas, examples of the decoy documents observed is given in Table 1.

Of course, being named in a decoy document doesn't mean any of these organizations have been attacked themselves or are involved in the attacks: the MuddyWater actors are abusing the trust these organizations' names and/or logos command for their malicious purposes.

Month	File Name or Decoy Document Theme	Suspected Target Region
Nov 2017	The NSA Telenor.doc	Unknown Pakistan
Oct 2017	Circulars.doc dollar.doc Pakistan Federal Investigation Agency CV of Middle Eastern Civil Servant	Turkey Pakistan
Sep 2017	Iraq National Intelligence Service Kaspersky Security solution 2017.doc	Iraq
Aug 2017	Arab Emirate سری.docm Iraq Commission of Integrity	Arab Emirates
Jul 2017	Requirements of the Sago.doc CommIT-Document.doc Confidential letters.doc	Saudi Arabia Arab Emirates Pakistan
Jun 2017	Iraq Kurdistan Regional Government RFP_VOIP.doc	Iraq

May 2017	RFP.doc Requirement.doc Iraq Kurdistan Regional Government	Georgia Iraq
Mar 2017	court.doc	Georgia
Feb 2017	CERT-Audit-20172802-GEO.xls	Georgia

Table 1 – Examples of the lure documents observed in the MuddyWater attacks.

All of these documents we observed and outlined above are related via:

- Shared C2 infrastructure.
- Use of the non-public PowerShell backdoor previously described by Morphisec and MalwareBytes (which we refer to as POWERSTATS).
- Shared attributes of the malicious documents used in attacks.
- Shared attributes as to how the documents were delivered.

Based on these connections we can be confident that all the files and infrastructure we give in our appendices are related, since more than one of these can be used to link each of the samples discussed in each case.

I download my tools from GitHub, and so do my victims.
The tools used by the MuddyWater attackers have been well documented by the previously cited research and a common theme of previous reporting was the open source nature of much of the toolset used by MuddyWater: Meterpreter, Mimikatz, Lazagne, Invoke-Obfuscation etc.. In some of their recent attack documents, the attackers also used GitHub as a hosting site for their custom backdoor, POWERSTATS. Specifically, the following GitHub repositories appear to be controlled by the MuddyWater threat actor(s):

- [unknown SHA256]
    - Downloads payload from: hxxps://raw.githubusercontent[.]com/F0R3X/BrowserFontArabic/master/ArabicBrowserFont.exe
- [unknown SHA256]
    - Downloads payload from: hxxps://raw.githubusercontent[.]com/F0R3X/BrowserFontArabic/master/FontArabic.exe

- 9b5e36bb7518a9e333c31d09b589102f89e3425571dd434820ab3c437dc4e0d9 (and several others)
    - Downloads payload from: hxxps://raw.githubusercontent[.]com/ReactDeveloper2017/react/master/src/test/test.js

Interestingly, both profiles were populated with forked repositories to give them an air of legitimacy as shown in figure 2. The POWERSTATS malware was compiled as an exe using PS2EXE. However, this was a minor

anomaly, as it was only seen in this case: raw scripts being used in all other cases.

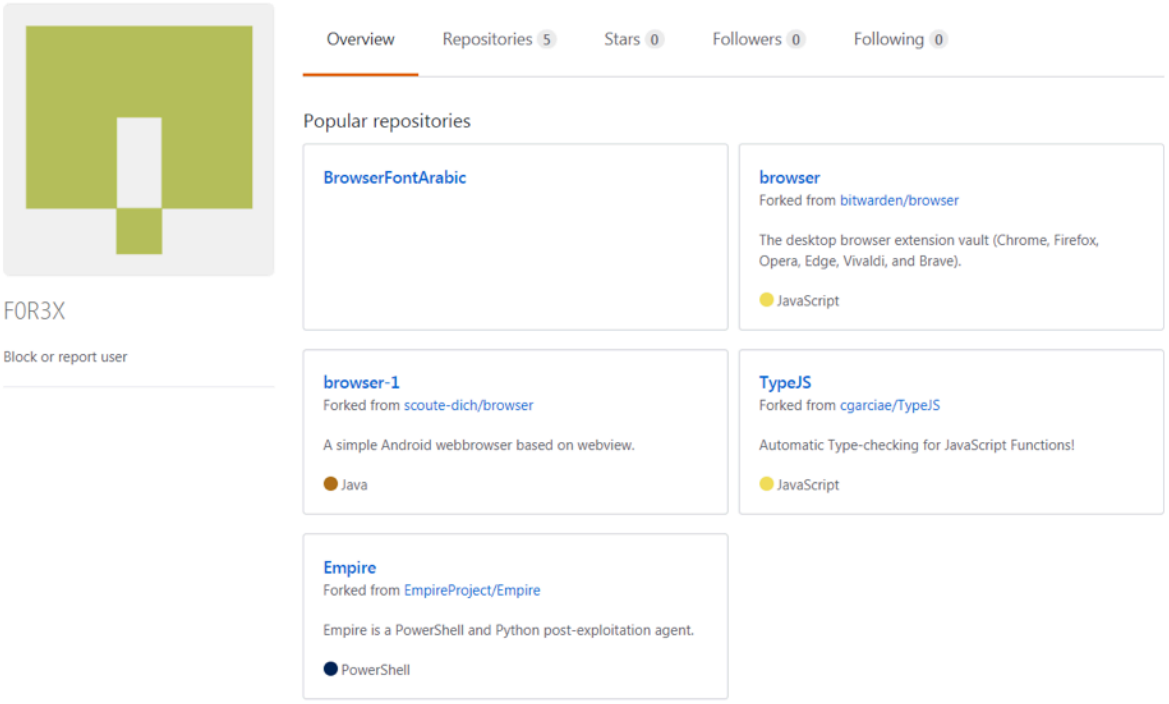

Figure 2 – The GitHub profile for F0R3X containing both legitimate forked code and the binaries created by the attacker. Note that the username could be a small joke on the attackers' part regarding the attribution to FIN7.

Pwn one to pwn them all

In some of the instances we observed what appeared to be compromised accounts at third party organizations sending the malware. In one case, the attackers sent a malicious document which was nearly identical to a legitimate attachment which we observed later being sent to the same recipient. This indicates that the attackers stole and modified a legitimate document from the compromised user account, crafted a malicious decoy Word macro document using this stolen document and sent it to the target recipient who might be expecting the email from the original account user before the real sender had time to send it.

This targeting of third party organizations to attack further targets is a risky move on the attackers' part, as it potentially reveals their activity within the compromised third party organizations to the new target (those receiving the malicious documents

Making sense of MuddyWater

When we looked at the cluster of activity which consisted of what appeared to be espionage-focused attacks in the Middle East, we were somewhat confused as the previous public reporting had attributed these attacks to FIN7. FIN7 is a threat actor group that is financially motivated with targets in the restaurant, services and financial sectors. Following the trail of existing public reporting, the tie to FIN7 is essentially made based on a download observed from a MuddyWater C2, of a non-public tool "DNSMessenger".

For example, Morphisec wrote:

"Later in our investigation, the same command server also delivered a variant of the DNS messenger similar to

that described by Talos. The domain names differed but the script adheres to the same logic (including the logic function)."

The DNSMessenger malware is an obfuscated and customized version of the popular DNS_TXT_PWNAGE.ps1 script available on GitHub and is also referred to by FireEye as POWERSOURCE. The use of the DNSMessenger tool appears primarily linked to FIN7, with no other samples being attributable to MuddyWater.

This led us to query the relationship between the newer attacks we were looking at and the alleged FIN7 link. As part of this research, we came up with the following hypotheses along with their likelihoods, and a rationale for each one.

1) The FIN7 threat actor is also involved in espionage in the Middle East - Unlikely

Whilst this may seem an attractive hypothesis to some, there are aspects on the technical side that simply don't add up. Primarily, there are significant disparities between FIN7 and MuddyWater, specifically in terms of:

- Malware unique to FIN7, or commonly used by them has not yet been seen in any MuddyWater investigations (except for the single observation of the DNSMessenger sample)
- Other non-public malware and tools used by MuddyWater have not been observed in our FIN7 investigations.
- From an infrastructure point of view there is no overlap between the two sets of activity, the only overlap is the use of the unique tool "DNSMessenger"

When these points are considered together in conjunction with the significant difference in targeting they make a strong case for classifying this activity as distinct from FIN7 activity.

2) The DNSMessenger malware is a shared tool, used by FIN7, MuddyWater and perhaps other groups - Unlikely

We have attempted to find examples of code available in public data sources that would generate the variation of the DNSMessenger malware and had little luck in doing so. Even though the code for DNSMessenger is publicly available following research into attackers published by 3rd parties, attackers would have to write the corresponding server side to use it, and as such they may well choose to use the public DNS_TXT_Pwnage.ps1 script instead.

Despite this, based on the chain of analysis above we cannot discount the notion that DNSMessenger is shared by multiple attackers, including FIN7 and MuddyWater.

3) There was a mistake in the original Morphisec analysis which linked these attacks to FIN7 - Possible

Little detail is given on the nature of how the connection between DNSMessenger and MuddyWater was discovered it isn't possible for us to verify this link.

4) The attackers realized they were under investigation and planted a false flag - Possible

The attackers realized they were under investigation and planted a false flag on their C2 server, uploading a copy of the FIN7 DNSMessenger code which had been previously mentioned (and was since publicly available) by FireEye and delivering it to researchers to trick them into mis-attributing the campaign.

Indeed, the sample shared by Morphisec on PasteBin is identical to the one dropped by the sample discussed in the FireEye FIN7 SEC campaign blog except for the final line.

Final thoughts

Whilst we could conclude with confidence that the attacks discussed in this article are not FIN7 related, we were not able to answer many of our questions about the MuddyWater attacks. We are currently unable to make a firm

conclusion about the origin of the attackers, or the specific types of information they seek out once on a network. In any case we will continue to track their activities to provide protections for our customers.

We hope the analysis presented shows the importance of drawing your own conclusions based on the data available to you, not just taking the conclusions given in the public domain at face value. This is especially true when actors who rely on slightly modified (and publicly available) open source tools are in play. Copycat threat actors can easily mimic attackers who use open source tools which can confuse attribution efforts meaning more than one aspect of the attacks observed must be considered when clustering.

On top of this, whilst the vast majority of threat analysis in the public domain is repeatable and correct, in some cases it can be difficult to verify the analysis available. When it is hard to reproduce the analysis the confidence in any conclusions drawn must be lower than it would otherwise be, since you cannot know for sure that what is stated is true.

Palo Alto Networks customers are protected from this threat in the following ways:

- WildFire and Traps detect all the malware supported in this report as malicious.
- Traps customers can deploy Heuristic methods to detect attacks that use these techniques.
- C2 domains used by the attackers are blocked via Threat Prevention.

AutoFocus customers can monitor ongoing activity from the threats discussed in this report by looking at the following tags:

- MuddyWater
- PowerStats
- LazaGne
- DNSMessenger
- FIN7

Appendix A – C2 Addresses

148.251.204[.]131
144.76.109[.]88
138.201.75[.]227

Compromised Legitimate Sites

106[.]187[.]38[.]21
arbiogaz[.]com
azmwn[.]suliparwarda[.]com
bangortalk[.]org[.]uk
best2[.]thebestconference[.]org
camco[.]com[.]pk
cbpexbrasilia[.]com[.]br
cgss[.]com[.]pk
diplomat[.]com[.]sa
feribschat[.]eu

ghanaconsulate[.]com[.]pk
magical-energy[.]com
mainandstrand[.]com
riyadhfoods[.]com
school[.]suliparwarda[.]com
suliparwarda[.]com
tmclub[.]eu
watyanagr[.]nfe[.]go[.]th
whiver[.]in
www[.]4seasonrentacar[.]com
www[.]akhtaredanesh[.]com
www[.]arcadecreative[.]com
www[.]armaholic[.]com
www[.]asan-max[.]com
www[.]autotrans[.]hr
www[.]dafc[.]co[.]uk
www[.]eapa[.]org
www[.]elev8tor[.]com
www[.]jdarchs[.]com
www[.]kunkrooann[.]com
www[.]mackellarscreenworks[.]com
www[.]mitegen[.]com
www[.]nigelwhitfield[.]com
www[.]pomegranates[.]org
www[.]ridefox[.]com
www[.]shapingtomorrowsworld[.]org
www[.]vanessajackson[.]co[.]uk
www[.]yaran[.]co
www[.]ztm[.]waw[.]pl
coa[.]inducks[.]org
mhtevents[.]com
skepticalscience[.]com
wallpapercase[.]com
www[.]spearhead-training[.]com

Appendix B – Related files

sha256	Overall Description
d2a0eec18d755d456a34865ff2ffc14e3969ea77f7235ef5dfc3928972d7960f	Loader script from 144.76.109[.]88
1421a5cd0566f4a69e7ca9cdefa380507144d7ed59cd22e53bfd25263c201a6f	MuddyWater Macro

4e3c7defd6f3061b0303e687a4b5b3cc2a4ae84cdc48706c65a7b1e53402efc0	MuddyWater Macro
8b96804d861ea690fcb61224ec27b84476cf3117222cca05e6eba955d9395deb	Lazagne
16985600c959f6267476da614243a585b1b222213ec938351ef6a26560c992db	PS2EXE PowerStats (GitHub)
cf87a2ac51503d645e827913dd69f3d80b66a58195e5a0044af23ea6ba46b823	PS2EXE PowerStats (GitHub)
3030d80cfe1ee6986657a2d9b76b626ea05e2c289dee05bd7b9553b10d14e4a1	Decoded PowerStats payload
99077dcb37395603db0f99823a190f50313dc4e9819462c7da29c4bc983f42fd	Lazagne Runner Script
1b60b7f9b0faf25288f1057b154413921a6cb373dcee43e831b9263c5b3077ce	MuddyWater Macro
2c8d18f03b6624fa38cae0141b91932ba9dc1221ec5cf7f841a2f7e31685e6a1	MuddyWater Macro
367021beedb3ad415c69c9a0e657dc3ed82b1b24a41a71537d889f5e2b7ca433	MuddyWater Macro
58282917a024ac252966650361ac4cbbbed48a0df7cab7b9a6329d4a04551c0d	MuddyWater Macro
58898648a68f0639c06bedc8242ca48bc6ec56f11ed40d00aa5fdda4e5553482	MuddyWater Macro
81523e0199ae1dc9e87d2b952642785bfbda6326f22e4c0794a19afdf001a9a3	MuddyWater Macro
90b66b3fef77962fbfda364a4f8799bfcc9ab73772026d7a8922a7cf5556a024	MuddyWater Macro
96101de2386e35bc5e38d32524a02c6c5ca7cc6624e656a629b2e0f1693a76fd	MuddyWater Macro
964aaf5d9b1c749df0a2df1f1b4193e5a643893f251e2d74b47663f895da9b13	MuddyWater Macro
97f9a83bc6bb1b3f5cb7ac9401f95265597bff796bb4901631d6fa2c79a48bdc	MuddyWater Macro
a3c1fd46177a078c4b95c744a24103df7d0a58cee1a3be92bc4cdd7dec1b1aa5	MuddyWater Macro
fcfbdffbcad731e0a5aad349215c87ed919865d66c287a6723fd8e2f896c5834	MuddyWater Macro
2bb1637c80f0a7df7260a8583beb033f4afbdd5c321ff5642bc8e1868194e009	MuddyWater Macro
58aec38e98aba66f9f01ca53442d160a2da7b137efbc940672982a4d8415a186	MuddyWater Macro
605fefc7829cfa41710e0b844084eab1f180fe513adc1d8f0f82501a154db0f4	MuddyWater Macro
e8a832b04dbdc413b71076754c3a0bf07cb7b9b61927248c482ddca32e1dab89	MuddyWater Macro
5d049bd7f478ea5d978b3c78f7f0afdf294a94f526fc20ffd6e33022d40d15ae	MuddyWater Macro
12a7898fe5c75e0b57519f1e7019b5d09f5c5cbe49c48ab91daf6fcc09ee8a30	MuddyWater Macro
2602e817a67949860733b3548b37792616d52ffd305405ccab0409bcfedc5d63	MuddyWater Macro

42a4d9527063f73004b049a093a34a4fc3b6ea9505cb9b50b895486cb2dca94b	MuddyWater Macro
5ed5fc6c6918ff6fa4eab7742c03d59155ca87e0fe12bac339f18928e2924a96	MuddyWater Macro
a2ad6bfc47c4f69a2170cc1a9fd620a68b1ebb474b7bdf601066e780e592222f	MuddyWater Macro
c23ece07fc5432ca200f3de3e4c4b68430c6a22199d7fab11916a8c404fb63dc	MuddyWater Macro
cb96cd26f36a3b1aacabfc79bbb5c1e0c9850b1c75c30aa498ad2d4131b02b98	MuddyWater Macro
ed2f9c9d5554d5248a7ad9ad1017af5f1bbadbd2275689a8b019a04c516eeec2	MuddyWater Macro
fe16543109f640ddbf3725e4d9f593de9f13ee9ae96c5e41e9cdccb7ab35b661	MuddyWater Macro
886e3a2f74bf8f46b23c78a6bad80c74fe33579f6fe866bc5075b034c4d5d432	MuddyWater Macro
8ec108b8f66567a8d84975728b2d5e6a2786c2ca368310cca55acad02bb00fa6	MuddyWater Macro
96d80ae577e9b899772a940b4941da39cf7399b5c852048f0d06926eb6c9868a	MuddyWater Macro
bb1a5fb87d34c63ade0ed8a8b95412ba3795fd648a97836cb5117aff8ea08423	MuddyWater Macro
d65e2086aeab56a36896a56589e47773e9252747338c6b59c458155287363f28	MuddyWater Macro
588cd0fe3ae6fbd2fa4cf8de8db8ae2069ea62c9eaa6854caedf45045780661f	MuddyWater Macro
917a6c816684f22934e2998f43633179e14dcc2e609c6931dd2fc36098c48028	MuddyWater Macro
db7bdd6c3ff7a27bd4aa9acc17dc35c38b527fb736a17d0927a0b3d7e94acb42	MuddyWater Macro
de6ce9b75f4523a5b235f90fa00027be5920c97a972ad6cb2311953446c81e1d	MuddyWater Macro
a6673c6d52dd5361afd96f8143b88810812daa97004f69661da625aaaba9363b	MuddyWater Macro
40a6b4c6746e37d0c5ecb801e7656c9941f4839f94d8f4cd61eaf2b812feaabe	MuddyWater Macro

Appendix C – Proxy URLs found from POWERSTATS samples from October 2017 onwards

hxxp://106[.]187[.]38[.]21/short_qr/work[.]php?c=
hxxp://arbiogaz[.]com/upload/work[.]php?c=
hxxp://azmwn[.]suliparwarda[.]com/wp-content/plugins/wpdatatables/panda[.]php?c=
hxxp://azmwn[.]suliparwarda[.]com/wp-content/themes/twentyfifteen/logs[.]php?c=
hxxp://bangortalk[.]org[.]uk/speakers[.]php?c=
hxxp://best2[.]thebestconference[.]org/ccb/browse_cat[.]php?c=
hxxp://camco[.]com[.]pk/Controls/data[.]aspx?c=
hxxp://cbpexbrasilia[.]com[.]br/wp-content/plugins/wordpress-seo/power[.]php?c=
hxxp://cbpexbrasilia[.]com[.]br/wp-includes/widgets/work[.]php?c=
hxxp://cgss[.]com[.]pk/data[.]aspx?c=
hxxp://diplomat[.]com[.]sa/wp-content/plugins/wordpress-importer/cache[.]php?c=

hxxp://feribschat[.]eu/logs[.]php?c=
hxxp://ghanaconsulate[.]com[.]pk/data[.]aspx?c=
hxxp://magical-energy[.]com/css[.]aspx?c=
hxxp://magical-energy[.]com/css/css[.]aspx?c=
hxxp://mainandstrand[.]com/work[.]php?c=
hxxp://riyadhfoods[.]com/css/edu[.]aspx?c=
hxxp://riyadhfoods[.]com/jquery-ui/js/jquery[.]aspx?c=
hxxp://school[.]suliparwarda[.]com/components/com_akeeba/work[.]php?c=
hxxp://school[.]suliparwarda[.]com/plugins/editors/codemirror/work[.]php?c=
hxxp://suliparwarda[.]com/includes/panda[.]php?c=
hxxp://suliparwarda[.]com/layouts/joomla/logs[.]php?c=
hxxp://suliparwarda[.]com/wp-content/plugins/entry-views/work[.]php?c=
hxxp://suliparwarda[.]com/wp-content/themes/twentyfifteen/work[.]php?c=
hxxp://tmclub[.]eu/clubdata[.]php?c=
hxxp://watyanagr[.]nfe[.]go[.]th/e-office/lib/work[.]php?c=
hxxp://watyanagr[.]nfe[.]go[.]th/watyanagr/power[.]php?c=
hxxp://whiver[.]in/power[.]php?c=
hxxp://www[.]4seasonrentacar[.]com/viewsure/data[.]aspx?c=
hxxp://www[.]akhtaredanesh[.]com/d/file/sym/work[.]php?c=
hxxp://www[.]akhtaredanesh[.]com/d/oschool/power[.]php?c=
hxxp://www[.]arcadecreative[.]com/work[.]php?c=
hxxp://www[.]armaholic[.]com/list[.]php?c=
hxxp://www[.]asan-max[.]com/files/articles/css[.]aspx?c=
hxxp://www[.]asan-max[.]com/files/articles/large/css[.]aspx?c=
hxxp://www[.]autotrans[.]hr/index[.]php?c=
hxxp://www[.]dafc[.]co[.]uk/news[.]php?c=
hxxp://www[.]eapa[.]org/asphalt[.]php?c=
hxxp://www[.]elev8tor[.]com/show-work[.]php?c=
hxxp://www[.]jdarchs[.]com/work[.]php?c=
hxxp://www[.]kunkrooann[.]com/inc/work[.]php?c=
hxxp://www[.]mackellarscreenworks[.]com/work[.]php?c=
hxxp://www[.]mitegen[.]com/mic_catalog[.]php?c=
hxxp://www[.]nigelwhitfield[.]com/v2/work[.]php?c=
hxxp://www[.]pomegranates[.]org/index[.]php?c=
hxxp://www[.]ridefox[.]com/content[.]php?c=
hxxp://www[.]shapingtomorrowsworld[.]org/category[.]php?c=
hxxp://www[.]vanessajackson[.]co[.]uk/work[.]php?c=
hxxp://www[.]yaran[.]co//wp-content/plugins/so-masonry/logs[.]php?c=
hxxp://www[.]yaran[.]co/wp-includes/widgets/logs[.]php?c=
hxxp://www[.]ztm[.]waw[.]pl/pop[.]php?c=
hxxps://coa[.]inducks[.]org/publication[.]php?c=
hxxps://mhtevents[.]com/account[.]php?c=

hxxps://skepticalscience[.]com/graphics[.]php?c=
hxxps://wallpapercase[.]com/wp-content/themes/twentyfifteen/logs[.]php?c=
hxxps://wallpapercase[.]com/wp-includes/customize/logs[.]php?c=
hxxps://www[.]spearhead-training[.]com//html/power[.]php?c=
hxxps://www[.]spearhead-training[.]com/work[.]php?c=
