Iranian Threat Group Updates Tactics, Techniques and Procedures in Spear Phishing Campaign

fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html

Breadcrumb

Threat Research

Sudeep Singh, Dileep Jallepalli

Mar 13, 2018

11 mins read

Introduction

From January 2018 to March 2018, through FireEye's Dynamic Threat Intelligence, we observed attackers leveraging the latest code execution and persistence techniques to distribute malicious macro-based documents to individuals in Asia and the Middle East.

We attribute this activity to TEMP.Zagros (reported by Palo Alto Networks and Trend Micro as MuddyWater), an Iran-nexus actor that has been active since at least May 2017. This actor has engaged in prolific spear phishing of government and defense entities in Central and Southwest Asia. The spear phishing emails and attached malicious macro documents typically have geopolitical themes. When successfully executed, the malicious documents install a backdoor we track as POWERSTATS.

One of the more interesting observations during the analysis of these files was the re-use of the latest AppLocker bypass, and lateral movement techniques for the purpose of indirect code execution. The IP address in the lateral movement techniques was substituted with the local machine IP address to achieve code execution on the system.

Campaign Timeline

In this campaign, the threat actor's tactics, techniques and procedures (TTPs) shifted after about a month, as did their targets. A brief timeline of this activity is shown in Figure 1.

Figure 1: Timeline of this recently observed spear phishing campaign

The first part of the campaign (From Jan. 23, 2018, to Feb. 26, 2018) used a macro-based document that dropped a VBS file and an INI file. The INI file contains the Base64 encoded PowerShell command, which will be decoded and executed by PowerShell using the command line generated by the VBS file on execution using WScript.exe. The process chain is shown in Figure 2.

Figure 2: Process chain for the first part of the campaign

Although the actual VBS script changed from sample to sample, with different levels of obfuscation and different ways of invoking the next stage of process tree, its final purpose remained same: invoking PowerShell to decode the Base64 encoded PowerShell command in the INI file that was dropped earlier by the macro, and executing it. One such example of the VBS invoking PowerShell via MSHTA is shown in Figure 3.

Figure 3: VBS invoking PowerShell via MSHTA

The second part of the campaign (from Feb. 27, 2018, to March 5, 2018) used a new variant of the macro that does not use VBS for PowerShell code execution. Instead, it uses one of the recently disclosed code execution techniques leveraging INF and SCT files, which we will go on to explain later in the blog.

Infection Vector

We believe the infection vector for all of the attacks involved in this campaign are macro-based documents sent as an email attachment. One such email that we were able to obtain was targeting users in Turkey, as shown in Figure 4.

Figure 4: Sample spear phishing email containing macro-based document attachment

The malicious Microsoft Office attachments that we observed appear to have been specially crafted for individuals in four countries: Turkey, Pakistan, Tajikistan and India. What follows is four examples, and a complete list is available in the Indicators of Compromise section at the end of the blog.

Figure 5 shows a document purporting to be from the National Assembly of Pakistan.

Figure 5: Document purporting to be from the National Assembly of Pakistan

A document purporting to be from the Turkish Armed Forces, with content written in the Turkish language, is shown in Figure 6.

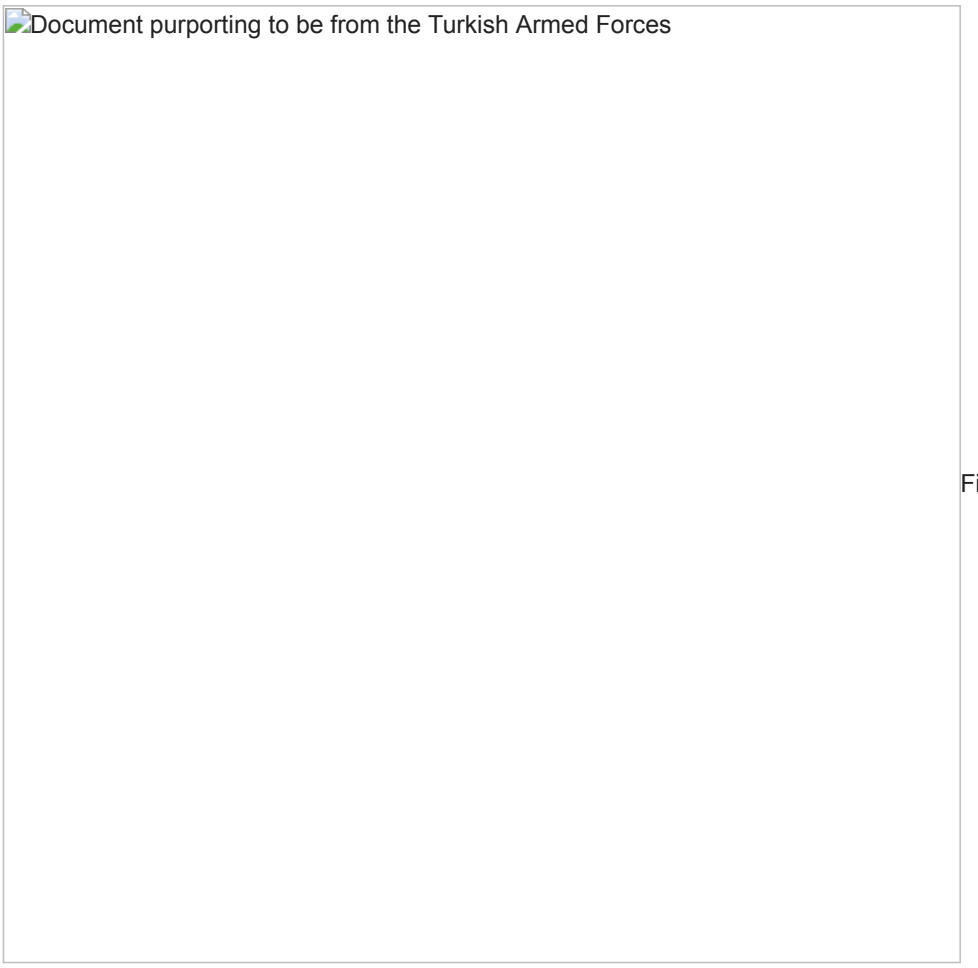

Figure 6: Document purporting to be from the Turkish Armed Forces

A document purporting to be from the Institute for Development and Research in Banking Technology (established by the Reserve Bank of India) is shown in Figure 7.

Figure 7: Document purporting to be from the Institute for Development and Research in Banking Technology

Figure 8 shows a document written in Tajik that purports to be from the Ministry of Internal Affairs of the Republic of Tajikistan.

Figure 8: Document written in Tajik that purports to be from the Ministry of Internal Affairs of the Republic of Tajikistan

Each of these macro-based documents used similar techniques for code execution, persistence and communication with the command and control (C2) server.

Indirect Code Execution Through INF and SCT

This scriptlet code execution technique leveraging INF and SCT files was recently discovered and documented in February 2018. The threat group in this recently observed campaign – TEMP.Zagros – weaponized their malware using the following techniques.

The macro in the Word document drops three files in a hard coded path: C:\programdata. Since the path is hard coded, the execution will only be observed in operating systems, Windows 7 and above. The following are the three files:

- **Defender.sct** – The malicious JavaScript based scriptlet file.
- **DefenderService.inf** – TheINF file that is used to invoke the above scriptlet file.
- **WindowsDefender.ini** – The Base64 encoded and obfuscated PowerShell script.

After dropping the three files, the macro will set the following registry key to achieve persistence:

\REGISTRY\USER\SID\Software\Microsoft\Windows\CurrentVersio
n\Run\"WindowsDefenderUpdater" = cmstp.exe /s c:\programdata\DefenderService.inf

Upon system restart, cmstp.exe will be used to execute the SCT file indirectly through the INF file. This is possible because inside the INF file we have the following section:

[UnRegisterOCXSection]
%11%\scrobj.dll,NI,c:/programdata/Defender.sct

That section gets indirectly invoked through the DefaultInstall_SingleUser section of INF, as shown in Figure 9.

Figure 9: Indirectly invoking SCT through the DefaultInstall_SingleUser section of INF

This method of code execution is performed in an attempt to evade security products. FireEye MVX and HX Endpoint Security technology successfully detect this code execution technique.

SCT File Analysis

The code of the Defender.sct file is an obfuscated JavaScript. The main function performed by the SCT file is to Base64 decode the contents of WindowsDefender.ini file and execute the decoded PowerShell Script using the following command line:

```
powershell.exe -exec Bypass -c
iex([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String((get-content
C:\\ProgramData\\WindowsDefender.ini)
```

The rest of the malicious activities are performed by the PowerShell Script.

PowerShell File Analysis

The PowerShell script employs several layers of obfuscation to hide its actual functionality. In addition to obfuscation techniques, it also has the ability to detect security tools on the analysis machine, and can also shut down the system if it detects the presence of such tools.

Some of the key obfuscation techniques used are:

- **Character Replacement:** Several instances of character replacement and string reversing techniques (Figure 10) make analysis difficult.

Figure 10: Character replacement and string reversing techniques

- **PowerShell Environment Variables:** Nowadays, malware authors commonly mask critical strings such as “IEX” using environment variables. Some of the instances used in this script are:
  - $eNv:puBLic[13]+$ENv:pUBLIc[5]+'x'
  - ($ENV:cOMsPEC[4,26,25]-jOin'')
- **XOR encoding:** The biggest section of the PowerShell script is XOR encoded using a single byte key, as shown in Figure 11.

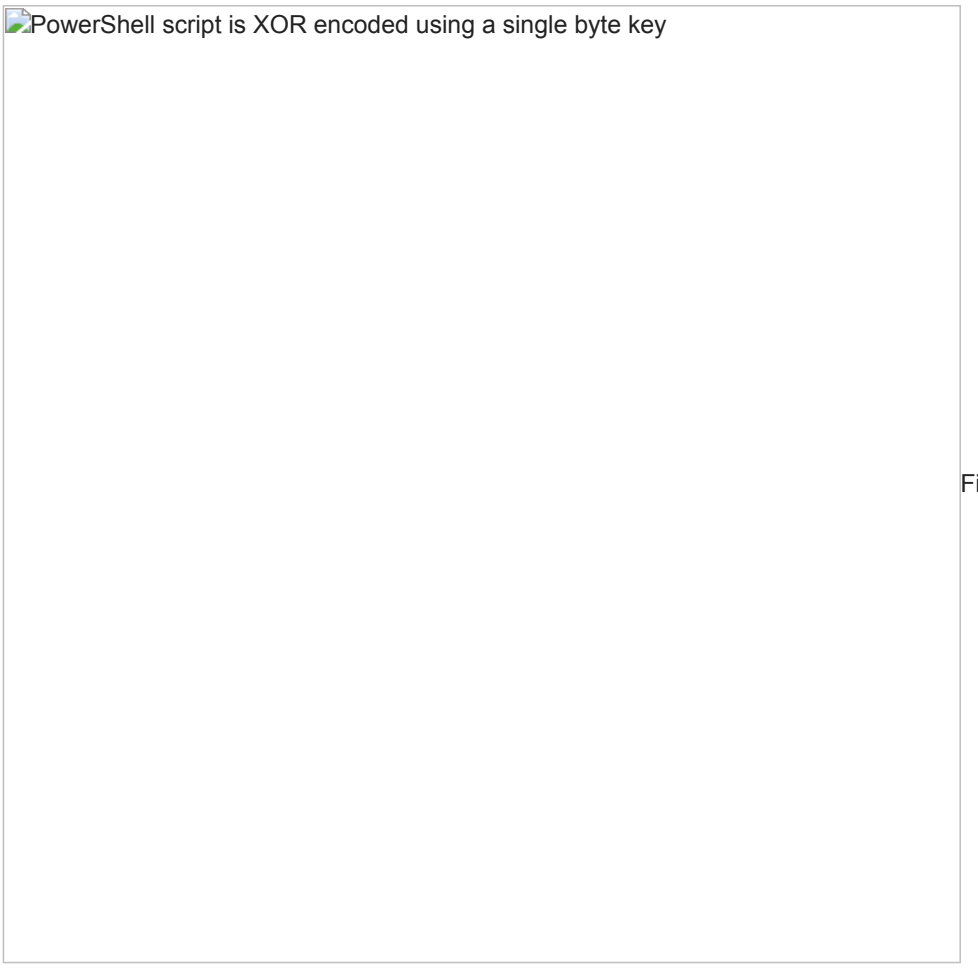

Figure 11: PowerShell script is XOR encoded using a single byte key

After deobfuscating the contents of the PowerShell Script, we can divide it into three sections.

Section 1

The first section of the PowerShell script is responsible for setting different key variables that are used by the remaining sections of the PowerShell script, especially the following variables:

- TEMpPAtH = "C:\ProgramData\" (the path used for storing the temp files)
- Get_vAIIdIP = https://api.ipify.org/ (used to get the public IP address of the machine)
- FIIENAmePATHP = WindowsDefender.ini (file used to store Powershell code)
- PRIVAtE = Private Key exponents
- PUbLIc = Public Key exponents
- Hklm = "HKLM:\Software\"
- Hkcu = "HKCU:\Software\"
- ValuE = "kaspersky"
- SYSID
- DrAGon_MidDLe = [array of proxy URLs]

Among those variables, there is one variable of particular interest, **DrAGon_MidDLe**, which stores the list of proxy URLs (detailed at the end of the blog in the Network Indicators portion of the Indicators of Compromise section) that will be used to interact with the C2 server, as shown in Figure 12.

Figure 12: DrAGon_MidDLe stores the list of proxy URLs used to interact with C2 server

Section 2

The second section of the PowerShell script has the ability to perform encryption and decryption of messages that are exchanged between the system and the C2 server. The algorithm used for encryption and decryption is RSA, which leverages the public and private key exponents included in Section 1 of the PowerShell script.

Section 3

The third section of the PowerShell script is the biggest section and has a wide variety of functionalities.

During analysis, we observed a code section where a message written in Chinese and hard coded in the script will be printed in the case of an error while connecting to the C2 server:

The English translation for this message is: “Cannot connect to website, please wait for dragon”.

Other functionalities provided by this section of the PowerShell Script are as follows:

Retrieves the following data from the system by leveraging Windows Management Instrumentation (WMI) queries and environment variables:

- IP Address from Network Adapter Configuration
- OS Name
- OS Architecture
- Computer Name
- Computer Domain Name
- Username

All of this data is concatenated and formatted as shown in Figure 13.

Figure 13: Concatenated and formatted data retrieved by PowerShell script

Register the victim's machine to the C2 server by sending the REGISTER command to the server. In response, if the status is OK, then a TOKEN is received from the C2 server that is used to synchronize the activities between the victim's machine and the C2 server.

While sending to the C2 server, the data is formatted as follows:

```
@{SYSINFO  = $get.ToString(); ACTION = "REGISTER";}
```

Ability to take screenshots.

Checks for the presence of security tools (detailed in the Appendix) and if any of these security tools are discovered, then the system will be shut down, as shown in Figure 14.

Figure 14: System shut down upon discovery of security tools

Ability to receive PowerShell script from the C2 server and execute on the machine. Several techniques are employed for executing the PowerShell code:

If command starts with “excel”, then it leverages DDEInitiate Method of Excel.Appilcation to execute the code:

If the command starts with “outlook”, then it leverages Outlook.Application and MSHTA to execute the code:

If the command starts with “risk”, then execution is performed through DCOM object:

File upload functionality.

Ability to disable Microsoft Office Protected View (as shown in Figure 15) by setting the following keys in the Windows Registry:

- DisableAttachmentsInPV
- DisableInternetFilesInPV
- DisableUnsafeLocationsInPV

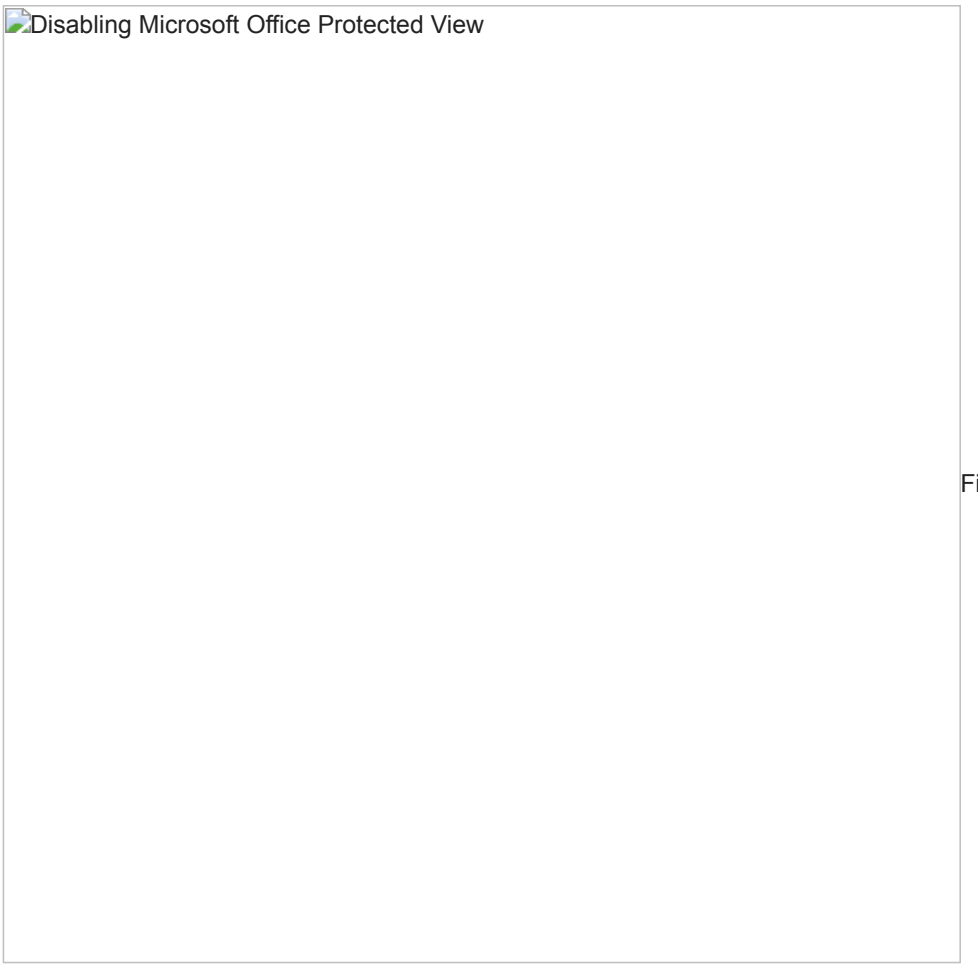

Figure 15: Disabling Microsoft Office Protected View

Ability to remotely reboot or shut down or clean the system based on the command received from the C2 server, as shown in Figure 16.

Figure 16: Reboot, shut down and clean commands

Ability to sleep for a given number of seconds.

The following table summarizes the main C2 commands supported by this PowerShell Script.

C2 Command	Purpose
reboot	Reboot the system using shutdown command
shutdown	Shut down the system using shutdown command
clean	Wipe the Drives, C:\, D:\, E:\, F:\
screenshot	Take a screenshot of the System
upload	Encrypt and upload the information from the system
excel	Leverage Excel.Application COM object for code execution
outlook	Leverage Outlook.Application COM object for code execution
risk	Leverage DCOM object for code execution

Conclusion

This activity shows us that TEMP.Zagros stays up-to-date with the latest code execution and persistence mechanism techniques, and that they can quickly leverage these techniques to update their malware. By combining multiple layers of obfuscation, they deter the process of reverse engineering and also attempt to evade security products.

Users can protect themselves from such attacks by disabling Office macros in their settings and also by being more vigilant when enabling macros (especially when prompted) in documents, even if such documents are from seemingly trusted sources.

Indicators of Compromise

Macro based Documents and Hashes

SHA256 Hash	Filename	Targeted Region
eff78c23790ee834f773569b52cddb01dc3c4dd9660f5a476af044ef6fe73894	na.doc	Pakistan
76e9988dad0278998861717c774227bf94112db548946ef617bfaa262cb5e338	Invest in Turkey.doc	Turkey
6edc067fc2301d7a972a654b3a07398d9c8cbe7bb38d1165b80ba4a13805e5ac	güvenlik yönergesi. .doc	Turkey
009cc0f34f60467552ef79c3892c501043c972be55fe936efb30584975d45ec0	idrbt.doc	India
18479a93fc2d5acd7d71d596f27a5834b2b236b44219bb08f6ca06cf760b74f6	Türkiye Cumhuriyeti Kimlik Kartı.doc	Turkey
3da24cd3af9a383b731ce178b03c68a813ab30f4c7c8dfbc823a32816b9406fb	Turkish Armed Forces.doc	Turkey
9038ba1b7991ff38b802f28c0e006d12d466a8e374d2f2a83a039aabcbe76f5c	na.gov.pk.doc	Pakistan
3b1d8dcbc8072b1ec10f5300c3ea9bb20db71bd8fa443d97332790b74584a115	MVD-FORM-1800.doc	Tajikistan
cee801b7a901eb69cd166325ed3770daffcd9edd8113a961a94c8b9ddf318c88	KEGM-CyberAttack.doc	Turkey
1ee9649a2f9b2c8e0df318519e2f8b4641fd790a118445d7a0c0b3c02b1ba942	IL-1801.doc	Turkey
aa60c1fae6a0ef3b9863f710e46f0a7407cf0feffa240b9a4661a4e8884ac627	kiyiemniyeti.doc	Turkey
93745a6605a77f149471b41bd9027390c91373558f62058a7333eb72a26faf84	TCELL-S1-M.doc	Tajikistan
c87799cce6d65158da97aa31a5160a0a6b6dd5a89dea312604cc66ed5e976cc9	egm-1.doc	Turkey
2cea0b740f338c513a6390e7951ff3371f44c7c928abf14675b49358a03a5d13	Connectel .pk.doc	Pakistan
18cf5795c2208d330bd297c18445a9e25238dd7f28a1a6ef55e2a9239f5748cd	gÃŸvenlik_yÃœnergesi_.doc	Turkey
153117aa54492ca955b540ac0a8c21c1be98e9f7dd8636a36d73581ec1ddcf58	MIT.doc	Turkey
d07d4e71927cab4f251bcc216f560674c5fb783add9c9f956d3fc457153be025	Gvenlik Ynergesi.doc	Turkey

af5f102f0597db9f5e98068724e31d68b8f7c23baeea536790c50db587421102	Gvenlik Ynergesi.doc	Turkey
5550615affe077ddf66954edf132824e4f1fe16b3228e087942b0cad0721a6af	NA	Turkey
3d96811de7419a8c090a671d001a85f2b1875243e5b38e6f927d9877d0ff9b0c	Anadolu GÃ¼neydoÄŸu Projesinde .doc	Turkey

Network Indicators

List of Proxy URLs

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

Appendix

Security Tools Checked on the Machine

win32_remote

win64_remote64

ollydbg

ProcessHacker

tcpview

autoruns

autorunsc

filemon

procmon

regmon

procexp

idaq

idaq64

ImmunityDebugger

Wireshark

dumpcap

HookExplorer

ImportREC

PETools

LordPE

dumpcap

SysInspector

proc_analyzer

sysAnalyzer

sniff_hit

windbg

joeboxcontrol

joeboxserver