



Confidential



Scope

Malware Monitoring for URL http://www.vfsglobal.com/Newzealand/

Limitations

- 1. The entire test was carried out with no prior knowledge of the systems and applications.
- 2. All test were carried out without any known credentials to systems and applications.
- 3. IndusGuard does not allowed to carry out any DoS attacks or to run any exploits which can affect systems availability.

Confidentiality

This document contains sensitive and/or confidential information, do not distribute, email, fax or transfer via any electronic mechanism without proper authorization. Information contained with in this document should be handled with appropriate caution. While reasonable attempts have been made to confirm the accuracy of the data contained herein, IndusGuard, assumes no liability for the completeness, use of, or conclusions drawn from such data.

Disclaimer

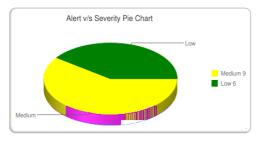
This, or any other, Security Audit cannot and does not guarantee security. IndusGuard makes no warranty or claim of any kind, whatsoever, about the accuracy or usefulness of any information provided herein. By using this information you agree that IndusGuard shall be held harmless in any event. IndusGuard makes this information available solely under its Terms of Service Agreement published at soc.indusguard.com.

Executive Summary

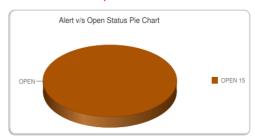
Total number of alert(s) identified are 15



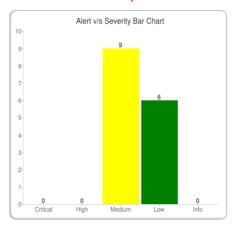
Alert v/s Severity Pie Chart



Alert v/s Open Status Pie Chart



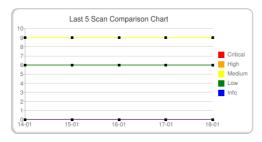
Alert v/s Severity Bar Chart



Alert Summary

| Severity | Total | |
|----------|-------|--|
| Critical | 0 | |
| High | 0 | |
| Medium | 9 | |
| Low | 6 | |
| Info | 0 | |

Comparison Chart



Comparison Summary

| Severity | 14 Jan | 15 Jan | 16 Jan | 17 Jan | 18 Jan |
|----------|-----------|-----------|-----------|-----------|-----------|
| Critical | 0 | 0 | 0 | 0 | 0 |
| High | 0 | 0 | 0 | 0 | 0 |
| Medium | 9 | 9 | 9 | 9 | 9 |
| Low | 6 | 6 | 6 | 6 | 6 |
| Info | 0 | 0 | 0 | 0 | 0 |



Alert Details

| Title | Total |
|---------------------|-------|
| Suspicious Change | 9 |
| External JavaScript | 6 |

URL Blacklist Status

| Google Google Blacklist | √ | SAFE |
|-------------------------|----------|------|
| Google Malware | √ | SAFE |
| Norton Safe Web | √ | SAFE |
| Mcafee | √ | SAFE |
| * PhishTank | √ | SAFE |
| Bing | √ | SAFE |
| Yahoo | √ | SAFE |

Alerts

Suspicious Change

Open Status: OPEN First Found: 2017-12-07

Link Placed On: http://www.vfsglobal.com/Newzealand/

Affected URL: http://www.vfsglobal.com/

Solution:

IndusGuard has detected suspicious change in the code. Please compare below mentioned actual and modified source codes, and take appropriate action.

Detail:

The URL header may be changed by an external entity. If this change is authentic then you can neutralize it.

Result:

Header Difference

<meta http-equiv="Content-Type" content="text/html; charset=utf-8">

<title>VFS Global</title>

<meta name="google-site-verification" content="xahrZyiOj65i2PlzNsN4t6IOfXLsvV4l8f8Zxz4PKog">

<meta name="description" content="VFS Global, Diplomatic Missions and Governments Worldwide">

<meta name="keywords" content="VFS Global, Diplomatic Missions and Governments Worldwide, visa services, visa services,</p> global visa services, visa processing service, visa services chennai, indian visa, gulf visa services, tourist visa, visa application, how to get visa, emirates visa services, visa services in india, , visa requirements, online visa application, visa online, visa services in Chennai, european visa, visas, international visa service, visa office, visa services, travel visa, global visa service, visa processing services, visa forms, emirates airlines visa service, visa services india, indian visa services, passport, us visa, visa agent, uk visa india, schengen visa, us visa application, student visa services, visa service agency, russian visa application form, canadian visa, indian embassy, saudi visa services, uk visa services in india, visa for America, visa india, visa help, worldwide visa services, chinese visa service, tourist visa for us, chinese visa form, passport & visa services, visa service provider, australian visa, visa service providers, how to get a visa, french visa, american visa, student visa, india visa, chinese visa application, marhaba visa services, chinese visa requirements, europe visa, british embassy, work visa, saudi visa, passport application, us travel visa, chinese business visa, american visa application form, us tourist visa, vfs visa services, indian visa service, types of visa, british visa, visa validity service, visa information, russian tourist visa, visa agency, visa application form, visa form, passport forms, chinese visa, global isas, visa and passport services, passport and visa services, business visa, international visa services, tourist visa to us, us visa services, chinavisa, types of visas, on line passport application, visa services ebsite, visa express, chinese visa application form, visa service provider list, american visa application, visa passport services, quick visa services, russian visa requirements, travel agent visa service,">

<meta name="viewport" content="width=device-width, initial-scale=1.0">

k rel="stylesheet" type="text/css" href="css/style.css">

k rel="stylesheet" type="text/css" href="css/website.css">

k rel="stylesheet" type="text/css" href="css/responsive.css">

<link rel="shortcut icon" type="image/x-icon" href="images/common/vfs.ico">

k rel="shortcut icon" type="image/x-icon" href="images/common/vfs.ico">

Page 4 of 17





```
<script type="text/javascript" src="js/ddaccordion.js"></script>
<script type="text/javascript" src="http://s
                                                                    <del>/jquery/1.4.2/jquery.min.js"></del>
        src="http://ajax.googleapis.com/ajax/libs/jquery/1.9.0/jquery.min.js"></script>
<!-- Google Tag Manager -->
new\ Date().getTime(), event: 'gtm.js'\}); var\ f=d.getElementsByTagName(s)[0], \\
j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:";j.async=true;j.src=
'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
})(window,document,'script','dataLayer','GTM-P9Q5746');</script>
<!-- End Google Tag Manager -->
<!-- Global site tag (gtag.js) - Google Analytics -->
<script async="" src="https://www.googletagmanager.com/gtag/js?id=UA-40516346-1"></script>
window.dataLayer = window.dataLayer || [];
function gtag(){dataLayer.push(arguments);}
gtag('js', new Date());
gtag('config', 'UA-40516346-1');
</script>
<script type="text/javascript">
ddaccordion.init({
headerclass: "menuheaders", //Shared CSS class name of headers group
contentclass: "menucontents", //Shared CSS class name of contents group
revealtype: "mouseover", //Reveal content when user clicks or onmouseover the header? Valid value: "click", or "mouseover"
mouseoverdelay: 200, //if revealtype="mouseover", set delay in milliseconds before header expands on Mouseover
collapseprev: true, //Collapse previous content (so only one open at any time)? true/false
defaultexpanded: [], //index of content(s) open by default [index1, index2, etc]. [] denotes no content.
onemustopen; false. //Specify whether at least one header should be open always (so never all headers closed)
animatedefault: false, //Should contents open by default be animated into view?
persiststate: false, //persist state of opened contents within browser session?
toggleclass: ["unselected", "selected"], //Two CSS classes to be applied to the header when it's collapsed and expanded,
respectively ["class1", "class2"]
togglehtml: ["none", "", ""], //Additional HTML added to the header when it's collapsed and expanded, respectively ["position",
"html1", "html2"] (see docs)
animatespeed: 500, //speed of animation: integer in milliseconds (ie: 200), or keywords "fast", "normal", or "slow"
oninit:function(expandedindices){ //custom code to run when headers have initalized
//do nothing
},
onopenclose:function(header, index, state, isuseractivated){ //custom code to run whenever a header is opened or closed
})
</script>
<script type="text/javascript" src="js/jquery.js"></script>
                   avascript" src="js/easySlider1.7.js"></script>
<script type="text/javascript">
$("#slider").easySlider({
auto: true,
continuous: true
});
});
</script>
<script type="text/javascript">
function menu(whatState)
{ //alert (whatState);
document.get Element By Id ("langu"). style. display=what State; \\
</script>
<script type="text/javascript">
function menu(whatState)
{ //alert (whatState);
document.getElementById ("langu").style.display=whatState;\\
</script>
<script language="javascript" type="text/javascript">
function senddata()
window.location = "search/search.asp?text=" + document.getElementById('search').value; \\
</script>
<script src="js/responsive.js" type="application/javascript"></script>
<!-- (max-width: 768px)]>
<script>
$(function(){
(".visa\_info\_panel").insertBefore(".watermark");
```

Page 5 of 17



});
</script>
<[endif]-->

Alert ID: 295919453 Found on: 2018-01-18 Severity:

Suspicious Change

Open Status: OPEN First Found: 2017-12-07

Link Placed On: http://www.vfsglobal.com/

Affected URL: http://www.vfsglobal.com/index.asp

Solution:

IndusGuard has detected suspicious change in the code. Please compare below mentioned actual and modified source codes, and take appropriate action.

Detail:

The URL header may be changed by an external entity. If this change is authentic then you can neutralize it.

Result

Header Difference

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>VFS Global</title>
<meta name="google-site-verification" content="xahrZyiOj65i2PlzNsN4t6IOfXLsvV4l8f8Zxz4PKog">
<meta name="description" content="VFS Global. Diplomatic Missions and Governments Worldwide">
<meta name="keywords" content="VFS Global, Diplomatic Missions and Governments Worldwide, visa services, visa service,
global visa services, visa processing service, visa services chennai, indian visa, gulf visa services, tourist visa, visa application,
how to get visa, emirates visa services, visa services in india, , visa requirements, online visa application, visa online, visa services
in Chennai, european visa, visas, international visa service, visa office, visa services, travel visa, global visa service, visa
processing services, visa forms, emirates airlines visa service, visa services india, indian visa services, passport, us visa, visa
agent, uk visa india, schengen visa, us visa application, student visa services, visa service agency, russian visa application form,
canadian visa, indian embassy, saudi visa services, uk visa services in india, visa for America, visa india, visa help, worldwide visa
services, chinese visa service, tourist visa for us, chinese visa form, passport & visa services, visa service provider, australian visa,
visa service providers, how to get a visa, french visa, american visa, student visa, india visa, chinese visa application, marhaba
visa services, chinese visa requirements, europe visa, british embassy, work visa, saudi visa, passport application, us travel visa,
chinese business visa, american visa application form, us tourist visa, vfs visa services, indian visa service, types of visa, british
visa, visa validity service, visa information, russian tourist visa, visa agency, visa application form, visa form, passport forms
chinese visa, global isas, visa and passport services, passport and visa services, business visa, international visa services, tourist
visa to us, us visa services, chinavisa, types of visas, on line passport application, visa services ebsite, visa express, chinese visa
application form, visa service provider list, american visa application, visa passport services, quick visa services, russian visa
requirements, travel agent visa service,">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
k rel="stylesheet" type="text/css" href="css/style.css">
k rel="stylesheet" type="text/css" href="css/website.css">
k rel="stylesheet" type="text/css" href="css/responsive.css">
k rel="shortcut icon" type="image/x-icon" href="images/common/vfs.ico">
k rel="shortcut icon" type="image/x-icon" href="images/common/vfs.ico">
<script type="text/javascript" src="js/ddaccordion.js"></script>
<script type="text/javascript" ==
        src="http://ajax.googleapis.com/ajax/libs/jquery/1.9.0/jquery.min.js"></script>
<!-- Google Tag Manager -->
<script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
new\ Date().getTime(), event:'gtm.js'\}); var\ f=d.getElementsByTagName(s)[0], \\
j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:";j.async=true;j.src=
'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
})(window,document,'script','dataLayer','GTM-P9Q5746');</script>
<!-- End Google Tag Manager -->
<!-- Global site tag (gtag.js) - Google Analytics -->
<script async="" src="https://www.googletagmanager.com/gtag/js?id=UA-40516346-1"></script>
<script>
window.dataLayer = window.dataLayer || [];
function gtag(){dataLayer.push(arguments);}
gtag('js', new Date());
gtag('config', 'UA-40516346-1');
</script>
```

Page 6 of 17

Scan Date: 2018-01-18

<script type="text/javascript">





```
ddaccordion.init({
headerclass: "menuheaders", //Shared CSS class name of headers group
contentclass: "menucontents", //Shared CSS class name of contents group
revealtype: "mouseover", //Reveal content when user clicks or onmouseover the header? Valid value: "click", or "mouseover"
mouseoverdelay: 200, //if revealtype="mouseover", set delay in milliseconds before header expands on Mouseover
collapseprev: true, //Collapse previous content (so only one open at any time)? true/false
defaultexpanded: [], //index of content(s) open by default [index1, index2, etc]. [] denotes no content.
onemustopen: false, //Specify whether at least one header should be open always (so never all headers closed)
animatedefault: false, //Should contents open by default be animated into view?
persiststate: false, //persist state of opened contents within browser session?
toggleclass: ["unselected", "selected"], //Two CSS classes to be applied to the header when it's collapsed and expanded,
respectively ["class1", "class2"]
togglehtml: ["none", "", ""], //Additional HTML added to the header when it's collapsed and expanded, respectively ["position",
"html1", "html2"l (see docs)
animatespeed: 500, //speed of animation: integer in milliseconds (ie: 200), or keywords "fast", "normal", or "slow"
oninit:function(expandedindices){ //custom code to run when headers have initalized
onopenclose:function(header, index, state, isuseractivated){ //custom code to run whenever a header is opened or closed
//do nothing
})
</script>
<script type="text/javascript" src="js/jquery.js"></script>
           <del>=="text/javascript"</del>src="js/easySlider1.7.js"></script>
<script type="text/javascript">
$(document).ready(function(){
$("#slider").easySlider({
auto: true,
continuous: true
});
});
</script>
<script type="text/javascript">
function menu(whatState)
{ //alert (whatState);
document.get Element By Id ("langu"). style. display=what State; \\
</script>
<script type="text/javascript">
function menu(whatState)
{ //alert (whatState);
document.getElementById ("langu").style.display=whatState;\\
</script>
<script language="javascript" type="text/javascript">
function senddata()
window.location = "search/search.asp?text=" + document.getElementById('search').value; \\
</script>
<script src="js/responsive.js" type="application/javascript"></script>
<!-- (max-width: 768px)]>
<script>
$(function(){
$(".visa_info_panel").insertBefore(".watermark");
</script>
<[endif]-->
```

```
Alert ID: 295919458 Found on: 2018-01-18

Suspicious Change

Open Status: OPEN First Found: 2017-12-11

Link Placed On: http://www.vfsglobal.com/
http://www.vfsglobal.com/about_us/company_profile.asp
```

Solution:

IndusGuard has detected suspicious change in the code. Please compare below mentioned actual and modified source codes, and take appropriate action.





Detail:

The URL header may be changed by an external entity. If this change is authentic then you can neutralize it.

Result

Header Difference

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>VFS Global</title>
k rel="stylesheet" type="text/css" href="../css/style.css">
k rel="stylesheet" type="text/css" href="../css/responsive.css">
k rel="shortcut icon" type="image/x-icon" href="../images/common/vfs.ico">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<script type="text/javascript" src="../js/ddaccordion.js"></script>
<script type="text/javascript" src="http://ajax.googleapis.com/ajax/libs/jquery/1.4.2/jquery.min.js"></script>
<!-- Google Tag Manager -->
<script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
new\ Date().getTime(), event:'gtm.js'\}); var\ f=d.getElementsByTagName(s)[0], \\
j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:";j.async=true;j.src=
'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
})(window,document,'script','dataLayer','GTM-P9Q5746');</script>
<!-- End Google Tag Manager -->
<!-- Global site tag (gtag.js) - Google Analytics -->
<script async="" src="https://www.googletagmanager.com/gtag/js?id=UA-40516346-1"></script>
window.dataLayer = window.dataLayer || [];
function gtag(){dataLayer.push(arguments);}
gtag('js', new Date());
gtag('config', 'UA-40516346-1');
</script>
<script type="text/javascript">
ddaccordion.init({
headerclass: "menuheaders", //Shared CSS class name of headers group
contentclass: "menucontents", //Shared CSS class name of contents group
revealtype; "mouseover". //Reveal content when user clicks or onmouseover the header? Valid value: "click", or "mouseover"
mouseoverdelay: 200, //if revealtype="mouseover", set delay in milliseconds before header expands onMouseover
collapseprev: true, //Collapse previous content (so only one open at any time)? true/false
defaultexpanded: [0], //index of content(s) open by default [index1, index2, etc]. [] denotes no content.
onemustopen: false, //Specify whether at least one header should be open always (so never all headers closed)
animatedefault: true, //Should contents open by default be animated into view?
persiststate: false, //persist state of opened contents within browser session?
toggleclass: ["unselected", "selected"], //Two CSS classes to be applied to the header when it's collapsed and expanded,
respectively ["class1", "class2"]
togglehtml: ["none", "", ""], //Additional HTML added to the header when it's collapsed and expanded, respectively ["position",
"html1", "html2"l (see docs)
animatespeed: 500, //speed of animation: integer in milliseconds (ie: 200), or keywords "fast", "normal", or "slow"
oninit:function(expandedindices){ //custom code to run when headers have initalized
onopenclose:function(header, index, state, isuseractivated){ //custom code to run whenever a header is opened or closed
//do nothing
})
</script>
<script type="text/javascript" src="../js/jquery.js"></script>
<script type="text/javascript" src="../js/easySlider1.7.js"></script>
<script type="text/javascript">
$(document).ready(function(){
$("#slider").easySlider({
auto: true,
continuous: true
});
});
</script>
<script type="text/javascript">
function menu(whatState)
{ //alert (whatState);
document.getElementById ("langu").style.display=whatState;\\
}
```



```
</script>
<script language="javascript" type="text/javascript">
function senddata()
{
window.location = "search/search.asp?text=" + document.getElementById('search').value;
}
</script>
<script src="../js/responsive.js" type="application/javascript"></script></script></script>
```

Alert ID: 295919459 Found on: 2018-01-18

Suspicious Change

Open Status: OPEN First Found: 2017-12-11

Link Placed On: http://www.vfsglobal.com/

Affected URL: http://www.vfsglobal.com/services_solutions/services_solutions.asp

Solution:

IndusGuard has detected suspicious change in the code. Please compare below mentioned actual and modified source codes, and take appropriate action.

Detail:

The URL header may be changed by an external entity. If this change is authentic then you can neutralize it.

<meta http-equiv="Content-Type" content="text/html; charset=utf-8">

Result:

<title>VFS Global</title>

Header Difference

```
k rel="stylesheet" type="text/css" href="../css/style.css">
k rel="stylesheet" type="text/css" href="../css/responsive.css">
k rel="shortcut icon" type="image/x-icon" href="../images/common/vfs.ico">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<script type="text/javascript" src="../js/ddaccordion.js"></script>
<\!\!\!\text{script type} = \text{"text/javascript" src} = \text{"http://ajax.googleapis.com/ajax/libs/jquery/1.4.2/jquery.min.js"} > <\!\!\!\text{script} > \text{-script} 
 <!-- Google Tag Manager -->
 new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
i=d.createElement(s),dl=l!='dataLayer'?'&l='+1:";i.async=true;i.src=
'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);\\
})(window,document,'script','dataLayer','GTM-P9Q5746');</script>
 <!-- End Google Tag Manager -->
 <!-- Global site tag (gtag.js) - Google Analytics -->
 <script async="" src="https://www.googletagmanager.com/gtag/js?id=UA-40516346-1"></script>
<script>
window.dataLayer = window.dataLayer || [];
function gtag(){dataLayer.push(arguments);}
gtag('js', new Date());
gtag('config', 'UA-40516346-1');
<script type="text/javascript">
ddaccordion.init({
headerclass: "menuheaders", //Shared CSS class name of headers group
contentclass: "menucontents", //Shared CSS class name of contents group
revealtype: "mouseover", //Reveal content when user clicks or onmouseover the header? Valid value: "click", or "mouseover"
mouseoverdelay: 200, //if revealtype="mouseover", set delay in milliseconds before header expands onMouseover
collapseprev: true, //Collapse previous content (so only one open at any time)? true/false
default expanded: \hbox{\tt [0], //index of content(s) open by default [index1, index2, etc]. \hbox{\tt [] denotes no content.}}
onemustopen: false, //Specify whether at least one header should be open always (so never all headers closed)
animatedefault: true, //Should contents open by default be animated into view?
persiststate: false, //persist state of opened contents within browser session?
toggleclass: ["unselected", "selected"], //Two CSS classes to be applied to the header when it's collapsed and expanded,
respectively ["class1", "class2"]
togglehtml: ["none", "", ""], //Additional HTML added to the header when it's collapsed and expanded, respectively ["position",
 "html1", "html2"] (see docs)
animatespeed: 500, //speed of animation: integer in milliseconds (ie: 200), or keywords "fast", "normal", or "slow"
oninit:function(expandedindices){ //custom code to run when headers have initalized
//do nothing
onopenclose:function(header, index, state, isuseractivated){ //custom code to run whenever a header is opened or closed
//do nothing
```

Page 9 of 17



```
})
</script>
<script type="text/javascript" src="../js/jquery.js"></script>
<script type="text/javascript" src="../js/easySlider1.7.js"></script>
<script type="text/javascript">
$(document).ready(function(){
$("#slider").easySlider({
auto: true,
continuous: true
});
});
</script>
<script type="text/javascript">
function menu(whatState)
{ //alert (whatState);
document.getElementById ("langu").style.display=whatState;\\
</script>
<script language="javascript" type="text/javascript">
function senddata()
window.location = "search/search.asp?text=" + document.getElementById('search').value;
</script>
<script src="../js/responsive.js" type="application/javascript"></script>
```

Alert ID: 295919460 Found on: 2018-01-18 Severity: M

Suspicious Change

Open Status: OPEN First Found: 2017-12-11

Link Placed On: http://www.vfsglobal.com/

Affected URL: http://www.vfsglobal.com/customisation_innovation/customisation.asp

Solution:

IndusGuard has detected suspicious change in the code. Please compare below mentioned actual and modified source codes, and take appropriate action.

Detail:

The URL header may be changed by an external entity. If this change is authentic then you can neutralize it.

Result:

Header Difference

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>VFS Global</title>
k rel="stylesheet" type="text/css" href="../css/style.css">
k rel="stylesheet" type="text/css" href="../css/responsive.css">
<link rel="shortcut icon" type="image/x-icon" href="../images/common/vfs.ico">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<script type="text/javascript" src="../js/ddaccordion.js"></script>
<!-- Google Tag Manager -->
new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:";j.async=true;j.src=
'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);\\
})(window,document,'script','dataLayer','GTM-P9Q5746');</script>
<!-- End Google Tag Manager -->
<!-- Global site tag (gtag.js) - Google Analytics -->
<script async="" src="https://www.googletagmanager.com/gtag/js?id=UA-40516346-1"></script>
window.dataLayer = window.dataLayer || [];
function gtag(){dataLayer.push(arguments);}
gtag('js', new Date());
gtag('config', 'UA-40516346-1');
<script type="text/javascript">
ddaccordion.init({
```

Page 10 of 17





```
headerclass: "menuheaders", //Shared CSS class name of headers group
contentclass: "menucontents", //Shared CSS class name of contents group
revealtype: "mouseover", //Reveal content when user clicks or onmouseover the header? Valid value: "click", or "mouseover"
mouseoverdelay: 200, //if revealtype="mouseover", set delay in milliseconds before header expands onMouseover
collapseprev: true, //Collapse previous content (so only one open at any time)? true/false
defaultexpanded: [0], //index of content(s) open by default [index1, index2, etc]. [] denotes no content.
onemustopen: false, //Specify whether at least one header should be open always (so never all headers closed)
animatedefault: true, //Should contents open by default be animated into view?
persist state: false, {\it //} persist state of opened contents within browser session?}
toggleclass: ["unselected", "selected"], //Two CSS classes to be applied to the header when it's collapsed and expanded,
respectively ["class1", "class2"]
togglehtml: ["none", "", ""], //Additional HTML added to the header when it's collapsed and expanded, respectively ["position",
"html1", "html2"l (see docs)
animatespeed: 500, //speed of animation: integer in milliseconds (ie: 200), or keywords "fast", "normal", or "slow"
oninit:function(expandedindices){ //custom code to run when headers have initalized
onopenclose:function(header, index, state, isuseractivated){ //custom code to run whenever a header is opened or closed
//do nothing
})
</script>
<script type="text/javascript" src="../js/jquery.js"></script>
<script type="text/javascript" src="../js/easySlider1.7.js"></script>
<script type="text/javascript">
$(document).readv(function(){
$("#slider").easySlider({
auto: true,
continuous: true
});
});
</script>
<script type="text/javascript">
function menu(whatState)
{ //alert (whatState);
document.getElementById("langu").style.display=whatState;
</script>
<script language="javascript" type="text/javascript">
function senddata()
window.location = "search/search.asp?text=" + document.getElementById('search').value; \\
</script>
<script src="../js/responsive.js" type="application/javascript"></script>
```

```
Alert ID: 295919461 Found on: 2018-01-18

Suspicious Change

Open Status: OPEN First Found: 2017-12-11

Link Placed On: <a href="http://www.vfsglobal.com/">http://www.vfsglobal.com/</a>

Affected URL: <a href="http://www.vfsglobal.com/our expertise/security practices.asp">http://www.vfsglobal.com/our expertise/security practices.asp</a>
```

Solution:

IndusGuard has detected suspicious change in the code. Please compare below mentioned actual and modified source codes, and take appropriate action.

Detail:

The URL header may be changed by an external entity. If this change is authentic then you can neutralize it.

Result:

Header Difference

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>VFS Global</title>
klink rel="stylesheet" type="text/css" href="../css/style.css">
klink rel="stylesheet" type="text/css" href="../css/responsive.css">
klink rel="stylesheet" type="text/css" href="../images/common/vfs.ico">
klink rel="shortcut icon" type="image/x-icon" href="../images/common/vfs.ico">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<script type="text/javascript" src="../js/ddaccordion.js"></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></scri
```

Page 11 of 17



```
<script type="text/javascript" src="http://ajax.googleapis.com/ajax/libs/jquery/1.4.2/jquery.min.js"></script>
<!-- Google Tag Manager --
new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:";j.async=true;j.src=
"https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);\\
})(window,document,'script','dataLayer','GTM-P9Q5746');</script>
<!-- End Google Tag Manager -->
<!-- Global site tag (gtag.js) - Google Analytics -->
<script async="" src="https://www.googletagmanager.com/gtag/js?id=UA-40516346-1"></script>
<script>
window.dataLayer = window.dataLayer || [];
function gtag(){dataLayer.push(arguments);}
gtag('js', new Date());
gtag('config', 'UA-40516346-1');
<script type="text/javascript">
ddaccordion.init({
headerclass: "menuheaders", //Shared CSS class name of headers group
contentclass: "menucontents", //Shared CSS class name of contents group
revealtype: "mouseover", //Reveal content when user clicks or onmouseover the header? Valid value: "click", or "mouseover"
mouseoverdelay: 200, //if revealtype="mouseover", set delay in milliseconds before header expands onMouseover
collapseprev: true, //Collapse previous content (so only one open at any time)? true/false
defaultexpanded: [0], //index of content(s) open by default [index1, index2, etc]. [] denotes no content.
onemustopen: false, //Specify whether at least one header should be open always (so never all headers closed)
animatedefault: true, //Should contents open by default be animated into view?
persiststate; false, //persist state of opened contents within browser session?
toggleclass: ["unselected", "selected"], //Two CSS classes to be applied to the header when it's collapsed and expanded,
respectively ["class1", "class2"]
togglehtml: ["none", "", ""], //Additional HTML added to the header when it's collapsed and expanded, respectively ["position",
"html1", "html2"] (see docs)
animatespeed: 500, //speed of animation: integer in milliseconds (ie: 200), or keywords "fast", "normal", or "slow"
oninit:function(expandedindices){ //custom code to run when headers have initalized
onopenclose:function(header, index, state, isuseractivated){ //custom code to run whenever a header is opened or closed
//do nothing
})
</script>
<script type="text/javascript" src="../js/jquery.js"></script>
<script type="text/javascript" src="../js/easySlider1.7.js"></script>
<script type="text/javascript">
$(document).ready(function(){
$("#slider").easySlider({
auto: true,
continuous: true
});
});
</script>
<script type="text/javascript">
function menu(whatState)
{ //alert (whatState);
document.getElementById("langu").style.display=whatState;
}
</script>
<script language="javascript" type="text/javascript">
function senddata()
window.location = "search/search.asp?text=" + document.getElementById('search').value;
</script>
<script src="../js/responsive.js" type="application/javascript"></script>
```

```
Alert ID: 295919462 Found on: 2018-01-18 Severity: Medium

Suspicious Change

Open Status: OPEN First Found: 2017-12-11

Link Placed On: http://www.vfsglobal.com/
Affected URL: http://www.vfsglobal.com/news_events/news_coverage.asp
```

Page 12 of 17



Solution:

IndusGuard has detected suspicious change in the code. Please compare below mentioned actual and modified source codes, and take appropriate action.

Detail

The URL header may be changed by an external entity. If this change is authentic then you can neutralize it.

Result:

Header Difference

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>VES Global</title>
k rel="stylesheet" type="text/css" href="../css/style.css">
k rel="stylesheet" type="text/css" href="../css/responsive.css">
k rel="shortcut icon" type="image/x-icon" href="../images/common/vfs.ico">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<script type="text/javascript" src="../js/ddaccordion.js"></script>
<script type="text/javascript" src="http://ajax.googleapis.com/ajax/libs/jquery/1.4.2/jquery.min.js"></script>
<!-- Google Tag Manager -->
<script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:";j.async=true;j.src=
'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
})(window,document,'script','dataLayer','GTM-P9Q5746');</script>
<!-- End Google Tag Manager -->
<!-- Global site tag (gtag.js) - Google Analytics -->
<script async="" src="https://www.googletagmanager.com/gtag/js?id=UA-40516346-1"></script>
window.dataLayer = window.dataLayer || [];
function gtag(){dataLayer.push(arguments);}
gtag('js', new Date());
gtag('config', 'UA-40516346-1');
</script>
<script type="text/javascript">
ddaccordion.init({
headerclass: "menuheaders", //Shared CSS class name of headers group
contentclass: "menucontents", //Shared CSS class name of contents group
revealtype: "mouseover", //Reveal content when user clicks or onmouseover the header? Valid value: "click", or "mouseover"
mouseoverdelay: 200, //if revealtype="mouseover", set delay in milliseconds before header expands onMouseover
collapseprev: true, //Collapse previous content (so only one open at any time)? true/false
defaultexpanded: [0], //index of content(s) open by default [index1, index2, etc]. [] denotes no content.
onemustopen: false, //Specify whether at least one header should be open always (so never all headers closed)
animatedefault: true. //Should contents open by default be animated into view?
persiststate: false, //persist state of opened contents within browser session?
toggleclass: ["unselected", "selected"], //Two CSS classes to be applied to the header when it's collapsed and expanded,
respectively ["class1", "class2"]
togglehtml: ["none", "", ""], //Additional HTML added to the header when it's collapsed and expanded, respectively ["position",
"html1", "html2"l (see docs)
animatespeed: 500, //speed of animation: integer in milliseconds (ie: 200), or keywords "fast", "normal", or "slow"
oninit:function(expandedindices){ //custom code to run when headers have initalized
onopenclose; function (header, index, state, is user activated) (//custom code to run whenever a header is opened or closed
//do nothing
})
<script type="text/javascript" src="../js/jquery.js"></script>
<script type="text/javascript" src="../js/easySlider1.7.js"></script>
<script type="text/javascript">
$(document).ready(function(){
$("#slider").easySlider({
auto: true,
continuous: true
});
});
</script>
<script type="text/javascript">
function menu(whatState)
{ //alert (whatState);
document.getElementById("langu").style.display=whatState;
```

Page 13 of 17



```
</script>
<script language="javascript" type="text/javascript">
function senddata()
{
window.location = "search/search.asp?text=" + document.getElementById('search').value;
}
</script>
<script src="../js/responsive.js" type="application/javascript"></script></script></script>
```

Alert ID: 295919549 Found on: 2018-01-18

Suspicious Change

Open Status: OPEN First Found: 2017-12-11

Link Placed On: http://www.vfsglobal.com/
Affected URL: http://www.vfsglobal.com/contact_us/overview.asp.

Solution:

IndusGuard has detected suspicious change in the code. Please compare below mentioned actual and modified source codes, and take appropriate action.

Detail:

The URL header may be changed by an external entity. If this change is authentic then you can neutralize it.

<meta http-equiv="Content-Type" content="text/html; charset=utf-8">

Result:

<title>VFS Global</title>

Header Difference

```
k rel="stylesheet" type="text/css" href="../css/style.css">
k rel="stylesheet" type="text/css" href="../css/responsive.css">
k rel="shortcut icon" type="image/x-icon" href="../images/common/vfs.ico">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<script type="text/javascript" src="../js/ddaccordion.js"></script>
<\!\!\!\text{script type} = \text{"text/javascript" src} = \text{"http://ajax.googleapis.com/ajax/libs/jquery/1.4.2/jquery.min.js"} > <\!\!\!\text{script} > \text{-script} 
 <!-- Google Tag Manager -->
 new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
i=d.createElement(s),dl=l!='dataLayer'?'&l='+1:";i.async=true;i.src=
'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);\\
})(window,document,'script','dataLayer','GTM-P9Q5746');</script>
 <!-- End Google Tag Manager -->
 <!-- Global site tag (gtag.js) - Google Analytics -->
 <script async="" src="https://www.googletagmanager.com/gtag/js?id=UA-40516346-1"></script>
<script>
window.dataLayer = window.dataLayer || [];
function gtag(){dataLayer.push(arguments);}
gtag('js', new Date());
gtag('config', 'UA-40516346-1');
<script type="text/javascript">
ddaccordion.init({
headerclass: "menuheaders", //Shared CSS class name of headers group
contentclass: "menucontents", //Shared CSS class name of contents group
revealtype: "mouseover", //Reveal content when user clicks or onmouseover the header? Valid value: "click", or "mouseover"
mouseoverdelay: 200, //if revealtype="mouseover", set delay in milliseconds before header expands onMouseover
collapseprev: true, //Collapse previous content (so only one open at any time)? true/false
default expanded: \hbox{\tt [0], //index of content(s) open by default [index1, index2, etc]. \hbox{\tt [] denotes no content.}}
onemustopen: false, //Specify whether at least one header should be open always (so never all headers closed)
animatedefault: true, //Should contents open by default be animated into view?
persiststate: false, //persist state of opened contents within browser session?
toggleclass: ["unselected", "selected"], //Two CSS classes to be applied to the header when it's collapsed and expanded,
respectively ["class1", "class2"]
togglehtml: ["none", "", ""], //Additional HTML added to the header when it's collapsed and expanded, respectively ["position",
 "html1", "html2"] (see docs)
animatespeed: 500, //speed of animation: integer in milliseconds (ie: 200), or keywords "fast", "normal", or "slow"
oninit:function(expandedindices){ //custom code to run when headers have initalized
//do nothing
onopenclose:function(header, index, state, isuseractivated){ //custom code to run whenever a header is opened or closed
//do nothing
```

Page 14 of 17



```
})
</script>
<script type="text/javascript" src="../js/jquery.js"></script>
<script type="text/javascript" src="../js/easySlider1.7.js"></script>
<script type="text/javascript">
$(document).ready(function(){
$("#slider").easySlider({
auto: true,
continuous: true
});
});
</script>
<script type="text/javascript">
function menu(whatState)
{ //alert (whatState);
document.getElementById ("langu").style.display=whatState;\\
</script>
<script language="javascript" type="text/javascript">
function senddata()
window.location = "search/search.asp?text=" + document.getElementById('search').value;
</script>
<script src="../js/responsive.js" type="application/javascript"></script>
<script src="../js/visa-info.js" type="application/javascript"></script>
```

Alert ID: 295919550 Found on: 2018-01-18 Severity:

Suspicious Change

Open Status: OPEN First Found: 2017-12-11

Link Placed On: http://www.vfsglobal.com/

Affected URL: http://www.vfsglobal.com/careers/our hr Philosophy.asp

Solution:

IndusGuard has detected suspicious change in the code. Please compare below mentioned actual and modified source codes, and take appropriate action.

Detail:

The URL header may be changed by an external entity. If this change is authentic then you can neutralize it.

Result

Header Difference

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>VFS Global</title>
 k rel="stylesheet" type="text/css" href="../css/style.css">
k rel="stylesheet" type="text/css" href="../css/responsive.css">
k rel="shortcut icon" type="image/x-icon" href="../images/common/vfs.ico">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<script type="text/javascript" src="../js/ddaccordion.js"></script>
  <script type="text/javascript" src="http://ajax.googleapis.com/ajax/libs/jquery/1.4.2/jquery.min.js"></script>
 <!-- Google Tag Manager -->
 new\ Date().getTime(), event:'gtm.js'\}); var\ f=d.getElementsByTagName(s)[0], leading the content of the cont
j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:"';j.async=true;j.src=
"https://www.googletagmanager.com/gtm.js?id="+i+dl;f.parentNode.insertBefore(j,f);" in the property of the p
})(window,document,'script','dataLayer','GTM-P9Q5746');</script>
 <!-- End Google Tag Manager -->
<!-- Global site tag (gtag.js) - Google Analytics -->
 <script async="" src="https://www.googletagmanager.com/gtag/js?id=UA-40516346-1"></script>
  <script>
window.dataLayer = window.dataLayer || [];
function gtag(){dataLayer.push(arguments);}
gtag('js', new Date());
gtag('config', 'UA-40516346-1');
</script>
<script type="text/javascript">
```

Page 15 of 17





```
ddaccordion.init({
headerclass: "menuheaders", //Shared CSS class name of headers group
contentclass: "menucontents", //Shared CSS class name of contents group
reveal type: "mouse over", // Reveal content when user clicks or on mouse over the header? Valid value: "click", or "mouse over" is a content when user clicks or on mouse over the header? Valid value: "click", or "mouse over" is a content when user clicks or on mouse over the header? Valid value: "click", or "mouse over" is a content when user clicks or on mouse over the header? Valid value: "click", or "mouse over" is a content when user clicks or on mouse over the header? Valid value: "click", or "mouse over" is a content when user clicks or on mouse over the header? Valid value: "click", or "mouse over" is a content when user clicks or on mouse over the header? Valid value: "click", or "mouse over the header?" Valid value: "click" or "mouse ove
mouseoverdelay: 200, //if revealtype="mouseover", set delay in milliseconds before header expands on Mouseover
collapseprev: true, //Collapse previous content (so only one open at any time)? true/false
defaultexpanded: [0], //index of content(s) open by default [index1, index2, etc]. [] denotes no content.
onemustopen: false, //Specify whether at least one header should be open always (so never all headers closed)
animatedefault: true, //Should contents open by default be animated into view?
persist state: false, {\it //} persist state of opened contents within browser session?}
toggleclass: ["unselected", "selected"], //Two CSS classes to be applied to the header when it's collapsed and expanded,
respectively ["class1", "class2"] togglehtml: ["none", "", ""], //Additional HTML added to the header when it's collapsed and expanded, respectively ["position",
"html1", "html2"] (see docs)
animatespeed: 500, //speed of animation: integer in milliseconds (ie: 200), or keywords "fast", "normal", or "slow"
oninit:function(expandedindices){ //custom code to run when headers have initalized
//do nothing
onopenclose:function(header, index, state, isuseractivated){ //custom code to run whenever a header is opened or closed
//do nothing
})
</script>
<script type="text/javascript" src="../js/jquery.js"></script>
<script type="text/javascript" src="../js/easySlider1.7.js"></script>
<script type="text/javascript">
$("#slider").easySlider({
auto: true,
continuous: true
});
});
</script>
 <script type="text/javascript">
function menu(whatState)
{ //alert (whatState);
document.get Element By Id ("langu"). style. display=what State;\\
</script>
<script language="javascript" type="text/javascript">
function senddata()
window.location = "search/search.asp?text=" + document.getElementById('search').value; \\
</script>
<script src="../js/responsive.js" type="application/javascript"></script>
```

Alert ID: 295919431 Found on: 2018-01-18

External JavaScript

Open Status: OPEN First Found: 2017-12-08

Link Placed On: http://www.yfsglobal.com/
Affected URL: https://www.googletagmanager.com/gtag/js

Solution:

IndusGuard has detected an external javascript that is hosted on some other internet location. Please analyze it and take an appropriate action.

Detail:

We have found an external javascript on this URL.

This is a possible way to inject malware in your website. If this javascript is legitimate then please add this alert to the whitelist.

Alert ID: 295919437 Found on: 2018-01-18

External JavaScript

Open Status: OPEN First Found: 2017-07-31

Link Placed On: http://www.vfsglobal.com/
Affected URL: https://www.images-home.com/image.js

Solution:

IndusGuard has detected an external javascript that is hosted on some other internet location. Please analyze it and take an appropriate action.

Page 16 of 17





Detail:

We have found an external javascript on this URL.

This is a possible way to inject malware in your website. If this javascript is legitimate then please add this alert to the whitelist.

Alert ID: 295919438 Found on: 2018-01-18 Severity: Low

External JavaScript

Open Status: OPEN First Found: 2017-12-07

Link Placed On: http://www.vfsglobal.com/

Affected URL: http://ajax.googleapis.com/ajax/libs/jquery/1.9.0/jquery.min.js

Solution:

IndusGuard has detected an external javascript that is hosted on some other internet location. Please analyze it and take an appropriate action.

Detail:

We have found an external javascript on this URL.

This is a possible way to inject malware in your website. If this javascript is legitimate then please add this alert to the whitelist.

Alert ID: 295919457 Found on: 2018-01-18 Severity: Low

External JavaScript

 Open Status:
 OPEN
 First Found:
 2017-07-31

 Link Placed On:
 http://www.vfsqlobal.com/about_us/company_profile.asp

 Affected URL:
 http://ajax.googleapis.com/ajax/libs/jquery/1.4.2/jquery.min.js

Solution:

IndusGuard has detected an external javascript that is hosted on some other internet location. Please analyze it and take an appropriate action.

Detail:

We have found an external javascript on this URL.

This is a possible way to inject malware in your website. If this javascript is legitimate then please add this alert to the whitelist.

Alert ID: 295921917 Found on: 2018-01-19 Severity: Low

External JavaScript

Open Status: OPEN First Found: 2017-08-01

Link Placed On: http://www.vfsglobal.com/austria/thailand/

Affected URL: http://ajax.googleapis.com/ajax/libs/jquery/1.4.3/jquery.min.js

Solution:

IndusGuard has detected an external javascript that is hosted on some other internet location. Please analyze it and take an appropriate action.

Detail:

We have found an external javascript on this URL.

This is a possible way to inject malware in your website. If this javascript is legitimate then please add this alert to the whitelist.

Alert ID: 295922273 Found on: 2018-01-19 Severity: Low

External JavaScript

Open Status: OPEN First Found: 2017-08-01

Link Placed On: http://www.vfsglobal.com/bulgaria/oman/

Affected URL: http://ajax.googleapis.com/ajax/libs/jquery/1.6.0/jquery.min.js

Solution:

IndusGuard has detected an external javascript that is hosted on some other internet location. Please analyze it and take an appropriate action.

Detail:

We have found an external javascript on this URL.

This is a possible way to inject malware in your website. If this javascript is legitimate then please add this alert to the whitelist.

Page 17 of 17

